

国际信息工程先进技术译丛

WILEY IEEE

低速无线个域网：实现基于IEEE 802.15.4的无线传感器网络（原书第3版）

Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors With IEEE802.15.4 (Third Edition)

[美] José A.Gutiérrez
[德] Ludwig Winkel
[美] Edgar H.Callaway,Jr.
[美] Raymond L.Barrett,Jr. 著

王泉 陈德基 魏逸鸿 韩松 译

IEEE官方出版，全面讲解IEEE 802.15.4标准
ZigBee联盟主席Bob Heile
HART通信基金会执行总监Ron Helson 联合推荐



机械工业出版社
CHINA MACHINE PRESS

国际信息工程先进技术译丛

低速无线个域网：实现基于 IEEE 802.15.4 的无线传感器网络（原书第3版）

［美］ José A. Gutiérrez

［德］ Ludwig Winkel

［美］ Edgar H. Callaway Jr. 著

［美］ Raymond L. Barrett Jr.

王泉 陈德基 魏逸鸿 韩松 译



机 械 工 业 出 版 社

IEEE 802. 15. 4 标准是物联网中最受欢迎、应用最广泛、最核心的技术。本书是 IEEE 官方出版的第一本关于“低速无线个域网”和“IEEE 802. 15. 4 标准”的书籍，是第一本关于协议标准本身系统开发和应用性的书籍。本书剖析了各种关键技术，介绍了工业无线领域的研究热点。

本书适合工业无线领域、物联网领域的从业人员、科研人员和高等院校相关专业师生阅读参考。

图书在版编目（CIP）数据

低速无线个域网：实现基于 IEEE 802. 15. 4 的无线传感器网络：原书第 3 版/（美）古铁雷兹等著；王泉等译. —北京：机械工业出版社，2014. 12

（国际信息工程先进技术译丛）

书名原文：Low - rate wireless personal area networks, third edition

ISBN 978-7-111-48481-3

Ⅰ. ①低… Ⅱ. ①古…②王… Ⅲ. ①无线电通信 - 传感器 - 研究 Ⅳ. ①TP212

中国版本图书馆 CIP 数据核字（2014）第 260933 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：林 桢 责任编辑：林 桢

版式设计：赵颖喆 责任校对：刘秀芝

封面设计：马精明 责任印制：李 洋

三河市宏达印刷有限公司印刷

2015 年 2 月第 1 版第 1 次印刷

169mm × 239mm · 11. 75 印张 · 223 千字

0001—2500 册

标准书号：ISBN 978 - 7 - 111 - 48481 - 3

定价：59. 80 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务

服务咨询热线：010 - 88361066

读者购书热线：010 - 68326294

010 - 88379203

网络服务

机工官网：www. cmpbook. com

机工官博：weibo. com/cmp1952

金书网：www. golden - book. com

教育服务网：www. cmpedu. com

封面无防伪标均为盗版

译　者　序

物联网技术在我国的发展如火如荼，而IEEE 802.15.4标准是物联网中最受欢迎、应用最广泛、最核心的技术。基于IEEE 802.15.4标准的低速无线个域网（LR－WPAN）是为机器设备间低成本、超低功耗、短距离无线通信而设计的网络。近年来，LR－WPAN的标准和技术受到了学术界和工业界的广泛关注，也涌现出了一批LR－WPAN系统、应用实例等，许多工业界的用户、工程师、学者等期望能更全面、深入地了解该技术。本书是IEEE官方出版的第一本关于“低速无线个域网”和“IEEE 802.15.4标准”的书籍。本书详细地介绍了LR－WPAN系统，是一本关于协议标准本身系统开发和应用性的书籍，是一本剖析LR－WPAN技术及应用层面的指导性书籍。通过阅读该书，工业界的工程师能更深入地掌握该技术，有利于其丰富LR－WPAN系统开发经验及产品开发经验；工业界的用户也能更全面地理解该技术及应用，有利于其在各种应用领域采用该无线技术；向学术界介绍工业无线领域的潜在研究热点，有利于其拓展和提升学术研究成果。

本书共分4个部分、共计13个章节。首先，本书的“第3版引言和最新信息”部分介绍了IEEE 802.15.4系列标准的最新进展。第1部分简述低速无线个域网及其应用；第2部分详细剖析基于IEEE 802.15.4技术的低速无线个域网中的各种关键技术。第3部分讲述系统设计方面需要考虑的问题以及在实际应用中可能面临的问题。第4部分简要介绍了WirelessHART系统及其应用，并剖析了WirelessHART中的一些关键技术以及安全问题。

本书由王泉、陈德基、魏逸鸿、韩松翻译，阳书贵参与了本书部分图表的绘制。由于译者的水平有限，再加上时间上的限制，本书的翻译难免存在不妥之处，敬请广大读者批评指正，译者在此深表谢意。

谨以此书献给所有关心、支持和帮助过我的人们！

译　者

2014年11月

推 荐 序

IEEE 标准协会提供了一个名为 IEEE Get 802® 的项目。该项目允许 IEEE 802® 标准在被公开六个月以后可以被公众下载使用。自 2003 年该标准首次公开后的两年间，IEEE 802.15.4™标准是继 IEEE 802.11™和 IEEE 802.3™标准之后下载量排第三的标准。在 ZigBee 联盟官网上你可以下载到 ZigBee 规范，它是在 IEEE 802.15.4 基础上定义的，其每周的平均下载量稳定在500 次，显然 IEEE 802.15.4 颇受欢迎。我很高兴地看到低速个域网的首次引入搅动了市场。一本简明的指导性书籍是非常宝贵的，有利于开发者理解那些冗长的标准、市场定位应用领域以及现实世界中如何处理实际事务。本书做到了这些，而且它的第二版更是带领我们进入这样一个快速增长的市场。

本书的作者另辟蹊径完成了这项任务，不仅仅因为他们聪明机智、善于表达，同时也与他们最先参与标准的制订密不可分。IEEE 802.15 工作组是为了开发一个低速率无线通信标准的初始设想而启动的。几乎与此同时，蓝牙技术联盟宣布成立。这样，由于相信蓝牙技术可以满足传感器网络的技术需求，所以市场有一段时间变得比较混乱。直到 2000 年年末，人们清楚地意识到蓝牙技术对无线耳机应用是很有效的，但是无法满足传感器网络的要求（低成本、较长的电池寿命以及网状网络）。这样，对低速率传感器网络通信标准的进一步需求导致了 802.15 工作组的成立并起草了 IEEE 802.15.4 标准。

我很荣幸领导 IEEE 802.15 工作组的初期工作，José Gutiérrez 学习到了如何在工作组中做出自己的贡献，因此他成为了这个组的技术编辑。这给了他一个独特的视角来从各个方面理解该标准。另外，ED Callaway、Ray Barrett、Venkat Bahl 和 Kursat Kimyaciglu 在无线低数据速率和网状网络方面都有资深背景，同时也做出了很多的贡献。他们不知疲倦的工作成就了 IEEE 802.15.4 标准的技术基石。我无法想出谁可以比 José、ED 和 Ray 更胜任撰写该指导性书籍并且使其沿用至今。另外，ED 和 José 对 ZigBee 联盟的组建也做出了贡献。José 领导了 ZigBee 联盟项目管理办公室，ED 是 ZigBee 联盟董事会成员。他们到现在都依然在各个方面积极地推动该技术的发展和提高。

自从低速无线个域网的第一次修订版出现，很多不同目的的修订版也相继出现了。我们启动了一个叫作 IEEE 802.15.4a™的物理层修订版，目前在 IEEE 标准过程中处于最后投票阶段。我们也完成了 IEEE 802.15.4 标准的修订版，即发布的 IEEE 802.15.4™—2006 标准。这个修订版清除了 MAC 层里面的一些问题，实质

上提高了安全套件，在 sub-1GHz 频段加入了更高数据比率的调制模式。除了目前在美国和欧洲支持的一些频段外，我们也打算开始两个分别针对中国和日本的 sub-1GHz 频段的新修订版，即 IEEE 802.15.4c™和 IEEE 802.15.4d™。自从第一个修订版开始，ZigBee 联盟也公布了 ZigBee 规范，该规范在 IEEE 802.15.4 标准的基础上增加了网络堆栈和应用层。ZigBee 规范自 2006 年 9 月起已经被下载超过了 35000 次。这些行为的结果是 IEEE 802.15.4 有可能在未来十年内成为地球上被最广泛部署的无线技术。

你是否想了解无线传感器网络市场，或者更直观地掌握 IEEE 802.15.4 标准以及其工作原理，这本书将是一个非常好的选择。谢谢各位，你们最好开始本书第 3 版的阅读计划。

Bob Heile

IEEE 802.15 项目主持

ZigBee 联盟主席

原书序

自从 IEEE 802. 15. 4 标准的最初版在 2003 年被发布后，它催化了一场研究无线传感网络及其应用的风暴。符合 IEEE 802. 15. 4 标准的低成本、低功耗、现有商用无线芯片和组件已经成为变革者，并且明确地建立起以 IEEE 802. 15. 4 为核心的无线传感网络技术。

有几个原因使我看到此书时很激动。我了解到本书作者都是此领域的专家并且钻研了多年。特别让我感到欣慰的是他们选取了 WirelessHART 作为第三版的关键特色。作者清晰地展示了 IEEE 802. 15. 4 标准的发展过程，并将以 IEEE 802. 15. 4 技术为基础的 WirelessHART 作为一个成功的产品案例进行了阐述。这本书可读性强，将会有助于对这些新兴标准的了解，并且有助于无线传感网络生态系统的成长。

使用 IEEE 802. 15. 4 标准的无线传感网络所具有的优势，促使了 HART 通信基金会在 2004 年末决定考虑扩展现有的工业通信标准以包含无线的能力。在 2005 年初，我们的无线工作组就致力于开发一种应用于工业过程自动化的无线通信标准。在 2007 年 9 月，我们成功地完成了该目标并发布了 WirelessHART 标准，它是一种简单、可靠、安全的无线通信标准，这种标准专门针对工业过程的测量和控制应用。在 2010 年 3 月，WirelessHART 成为了被国际电工委员会（IEC）批准的国际标准 IEC 62591。

WirelessHART 是基于 IEEE 802. 15. 4 技术并针对工业应用的无线传感网络技术。应用于工业过程自动化中的通信标准和系统要求特别高的可靠性、安全性和健壮性。WirelessHART 利用了 IEEE 802. 15. 4 标准来满足这些需求，并且正在利用无可匹敌的可靠性和安全性来改变工业无线通信系统。

无须赘言，我们对于 WirelessHART 标准及其带给工业的机遇、可能性和好处感到非常兴奋。WirelessHART 标准的发展离不开辛勤的工作，不屈不挠的精神，以及许多人和公司对于此标准发展和进步贡献的专业知识。

最后，我相信还有几件重要的事情值得提及：WirelessHART 不是针对所有应用的，其主要应用是工业过程测量和控制。我们不可能把 WirelessHART 设计成针对所有无线传感网络应用的通用标准。同时，WirelessHART 与 ZigBee 标准不是相互竞争的，这两种无线通信标准和技术对工业应用都很重要，但是它们的市场侧重点和性能优点却十分不同。

不论你是无线传感网络领域的新人，或者是想更深入理解 IEEE 802. 15. 4 标准

的工程师，还是已经有可能使用 IEEE 802.15.4 技术的人，这本书都会非常适合你。作者已经完成了相当出色的工作，我对于他们允许我做出此微薄的贡献表示感谢。

Ron Helson
执行总监
HART 通信基金会

作者简介



JoséA. Gutiérrez，爱默生公司电子技术总监，主持包括工业领域无线传感器网络应用等诸多技术开发工作。1991年获得位于委内瑞拉首都加拉加斯的西蒙玻利瓦尔大学电子工程专业的学士学位，2001年获得美国威斯康星大学电子工程专业硕士学位，并于2005年在该校获得博士学位。由于在IEEE LAN/MAN标准委员会的活跃表现，Gutiérrez博士于2000年成为IEEE 802.15™工作组第四任务组主编，关注低速无线个域网的发展情况。在IEEE 802.15.4标准成功发布以后，他协助创立了ZigBee联盟，从2003年到2005年年初担任项目经理，然后从2009年开始成为ZigBee联盟董事会的一员。如今，Gutiérrez博士为HART商业基金会和IEC的中间协调人，是专注于无线共存问题的IEC SC65C WG-17工作组的美国专家，同时也是这些组织的技术顾问。Gutiérrez博士在无线个域网和无线局域网领域有多项专利，在自动控制、人工智能和无线通信方面发表多篇论文。Gutiérrez博士还出版了一本有关机器视觉技术的书籍——《机器视觉和摄影测量领域的精确地理坐标定位：发现并实现最高精度》（Springer出版社2007出版）。Gutiérrez博士是IEEE高级会员和IEEE标准协会活跃会员。



Ludwig Winkel，1977年获得德国沙尔大学电工电子控制工程专业的硕士学位。同年11月进入位于德国卡尔斯鲁厄市的西门子股份公司，加入电子测量设备的研发团队。在该年，Ludwig革命性地将微控制器技术和大规模集成芯片引入到测量设备中。这项工作也带来了其他的研发工作，譬如他编写了一个操作系统，并以此为基础实现测试和测量。然后他成为了一个研发团队的负责人，负责开发闭环控制硬件设备和用于可编程序控制器（SIMATIC® PLC）的软件，之后带领分布式控制系统TELEPERM®的维护团队。Ludwig推进了新的分布式控制系统SIMATIC PLC7的开发，并写了两本关于系统设计的书，《SIMATIC软件——过程控制系统PCS7验证支持手册Ⅰ》和《SIMATIC软件——过程控制系统PCS7验证支持手册Ⅱ》。

从1992年起，Ludwig积极推进仪表控制系统标准的完善。他成为互操作系统

项目的一员，也是IEC下属委员会65C中负责过程控制与现场总线功能块的IEC SC65C WG6的一员。1999年，他加入西门子公司自动化部现场总线通信战略组。在该职位上他积极参与推动行业标准的发展，并成为无线共存工作组IEC SC65C WG17、现场总线维护团队IEC SC65C MT9、实时以太网工作组IEC SC65C WG11等的召集人，WirelessHART规范IEC SC65C W16（IEC 62591项目）、电子设备描述语言（EDDL）工作组IEC SC65E WG7、“工业自动化系统与集成——开放系统应用集成框架——第四部分：基于以太网的控制系统修订案1——工业以太网配置的参考说明书”ISO TC184SC5 WG7等的编辑，处理EDDL的ISA 104联合主席，IEC SC65E WG7联络官，IEEE 802.15.4e的编辑之一，ETSI ERM TG28项目TR102889-2起草人，德国国家现场总线委员会DKE K956副主席以及多个国家和国际组织的专家。



Edgar H. Callaway，于1979~1983年在佛罗里达州大学学习，获得数学专业学士学位和电机工程专业硕士学位，另外，他于1987年获得诺瓦（如今的诺瓦东南）大学工商管理学硕士，2002年获得佛罗里达亚特兰大学计算机工程博士学位。1984年他加入摩托罗拉公司，成为一名射频工程师，开发集群无线电产品。1990年，他转入摩托罗拉公司寻呼产品部，在这里他设计了寻呼收发机系统，并且担任摩托罗拉公司寻呼平台设计主管。在2000年Callaway博士进入摩托罗拉公司实验室，研究低功率无线网络并在IEEE 802.15.4低速率无线个域网标准的发展上起到重要作用。同时他作为摩托罗拉公司的代表进入了ZigBee联盟董事会，在ZigBee安全工作组占据了一席之地。2009年Callaway博士与人合伙创立了Sunrise Micro Devices公司，专门从事低电压、低功率无线系统的研发。Callaway博士是一名注册专业工程师（佛罗里达州），作为作者著有多本书籍，参与编著了专著的部分章节，并撰写了多篇论文，还拥有超过40项美国专利。因其对无线传感器网络和通信设备、系统上的低功耗设计技术做出了很大贡献，Callaway于近期成为了一名IEEE Fellow。



Raymond Louis Barrett，1966年获得凯斯理工学院电子电工学士学位，分别于1983年和1982年获得诺瓦（现在称为诺瓦东南）大学计算机科学硕士和工商管理学硕士学位，1990年获得佛罗里达亚特兰大大学（FAU）电子工程博士学位。1982~2001年期间，他先后担任过诺瓦大学、佛罗里达亚特兰大大学助理教授以及北佛罗里达大学副教授。1991年，在佛罗里达亚特兰大大学任教的同时，他加入了摩托罗拉公司寻呼产品组，在这里他首创性

地设计了许多低功耗的寻呼接收机电路。然后他加入了摩托罗拉公司实验室，成为核心技术人员，并对低功耗无线组件感兴趣。目前他担任美国研发分公司 CEO 一职，该公司提供专业的工程服务。他还是 Sun Cam 公司提供的继续教育课程中十一个单元的编写者，该课程是为满足在美国所有州的专业工程许可证而开设的。他也是新罕布什尔大学的客座教授，教授其感兴趣的超大规模集成电路设计。同时他也是一名注册专业工程师（佛罗里达州），并且拥有三十五项美国专利，发表了若干篇论文。

目　　录

第0章　第3版的介绍和更新

IEEE 802.15.4™标准是第一个也是仅有的无线射频技术，用于机器之间以及机器与人之间的通信，其应用领域包括住宅、商业以及工业。IEEE 802.15.4 标准允许无线传感和执行系统的创建以实现机器与机器间的通信，也可简单地称为无线传感器网络（WSN）。

无线传感器网络有几个独特的要求，使得它们不同于传统的无线通信技术。大部分无线传感器应用主要受以下一些因素的限制：功耗；技术性能要求（例如吞吐量、等待时间、可靠性和安全性）；以及其他挑战（例如成本和易用性）。针对这些问题，IEEE 802.15.4 技术定义了一个简单但是健壮的无线技术，并且可以通过上层通信协议的配置来满足一些特殊应用的要求。例如 ZigBee 技术主要针对的是住宅和商业应用，而 WirelessHART 技术针对的是工业应用。

自从 2003 年最初版本的 IEEE 802.15.4 标准公布以来，人们对低速无线个域网（LR - WPAN）和无线传感器网络的兴趣以指数方式增加。无线传感市场产生了一系列人才、公司、系统和集中解决特殊问题的应用工具。这些应用包括智能电网的家庭局域网、工业现场仪表连接、消费类电子通信设备、健康监测、商业环境中的状态监测和一些其他应用。

正如最初的设计，IEEE 802.15.4 标准成为了实现机器对机器通信应用的关键技术，也成为了其他技术想融入这个应用领域的基准。例如，目前正在发展中的新的低功耗蓝牙技术（以前叫作 WiBree），以及新引进的低功耗 802.11™系统，该系统可以实现对利用已有的 Wi - Fi 基础设施组建无线监控系统。这些技术为无线传感器网络的特殊应用场合做了补充。无论如何，在同等条件和设想下它们在与由 IEEE 802.15.4 支持的低功耗系统的竞争中占不了优势，其原因是 IEEE 802.15.4 设计的简易性。简易性就意味着简单和能够简易实现。在半导体世界，简易性也意味着更少的入口、更少的代码和更少的处理能力，所有这些都比其他已有的技术低一到二个数量级的功耗。当然，如此的低功耗则会造成更低吞吐量（低速率），更短传播距离和较少的特性，这将在本书的后面章节中解释。

另一个相关的动态是专有无线通信系统向 IEEE 802.15.4 无线电的使用转化。这些系统可以使用 IEEE 802.15.4 商业化的射频技术，该技术包括十几个供应商提供的、使用基于 IEEE 802.15.4 团体知识库的、丰富的功能集。

0.1 IEEE 802.15.4 标准的进化

随着2003年最初版本的发布，IEEE 802.15.4 标准持续发展，已经包括了一些新技术特点，从而实现了它在位置识别之类的新型专业应用中的使用，提高和增强了它在新市场中的使用，同时还支持在中国和日本新引入的无线传感网络频段，并且允许更简单的实现（比如灵活的时分多址（TDMA）与工业应用中的时隙信道跳频（TSCH）的合并）。图0-1形象化地展示了 IEEE 802.15.4 标准进化历程。

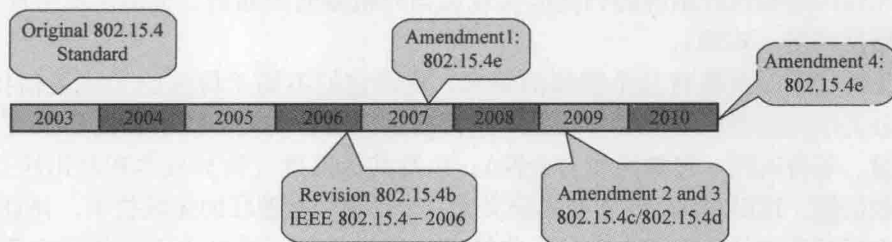


图0-1 IEEE 802.15.4 标准进化历程

1. IEEE 802.15.4—2006 修订版（IEEE 802.15.4b）

2006年6月，IEEE 标准协会通过了 IEEE 802.15.4—2003 版本的修订版，即 IEEE 802.15.4—2006。IEEE 802.15.4 的4b任务组制定了此修订版，其目的在于去除本标准中模棱两可的地方，同时对物理层（PHY）和媒体访问控制（MAC）层做了技术方面的改进。这个修订版中的物理层定义有了扩展，从而包括了新的可选的调制方案：

1）868/915MHz DSSS 物理层，其使用偏移四相移相键控（O-QPSK）调制方法。

2）868/915MHz 并行序列扩频（PSSS）物理层，其使用二进制相移键控（BPSK）和幅移键控（ASK）调制方法。

这两个新的物理层在868/915MHz频段提供更高的数据传输率，同时也增加了更多的信道。

2. 修订版1——IEEE 802.15.4a 标准

IEEE 802.15.4a 标准，在2007年8月通过，其通过增加支持精密测距和定位以及更高的总吞吐量的可选性能，从而扩大了 IEEE 802.15.4 标准家族。这样的改进是通过增加两个新的可选的物理层来完成的：

1）在3~5GHz、6~10GHz以及小于1GHz的频段的超宽带（UWB）物理层。这种物理层支持851kbit/s的无线强制性的数据传输率，以及可选的110kbit/s、6.81Mbit/s和27.24Mbit/s的数据传输率。

2）在2540MHz的线性调频扩频（CSS）物理层。该线性调频扩频物理层支持250kbit/s和1000kbit/s的无线数据传输率。

设计精密测距性能的目的是希望能够精确到1m或者更好的精度。

3. 修订版2——IEEE 802.15.4c标准

此修订版在2009年3月通过，增加了两个专门用来解决我国新开放的779~787MHz无线传感网络频段（也称为780MHz中国频段）的物理层：

1）为我国标准的无线媒体访问控制（MAC）定义的MPSK物理层。

2）为低速无线个域网设计的O-QPSK物理层规范。

4. 修订版3——IEEE 802.15.4d标准

此修订版也是在2009年3月19日通过的，其规定了两个可选的物理层以运行在日本的950MHz频段：

1）直接序列扩频（DSSS）物理层，使用BPSK调制方法。

2）一个使用高斯频移键控（GFSK）调制方法的物理层。

5. 修订版4——IEEE 802.15.4e标准

IEEE 802.15.4的4e任务组被授予的任务是为已有的IEEE 802.15.4—2006标准定义一个MAC层的修订方案。该修订方案的目标是增强并增加处理工业市场需求的能力。特别的，它定义了MAC层对时分多址（TDMA）和信道跳频的支持，而它们正是在工业设施中增加无线可靠性的关键参数。对IEEE 802.15.4e标准功能的详细技术解释在第4部分有介绍。

截止到2010年第一季度，IEEE 802.15.4e的标准化工作仍在进行中。

6. 修订版5——IEEE 802.15.4f标准

IEEE 802.15.4的4f任务组被授予的任务是定义一个新的无线物理层，以及对IEEE 802.15.4—2006的MAC层做相应的更新，要求MAC层能够双向地支持主动射频识别（RFID）系统和支持位置确定应用。截止到2010年第三季度，该修订方案的工作仍在进行中。

7. 修订版6——IEEE 802.15.4g标准

IEEE 802.15.4g标准尝试对标准做优化处理，从而为智能电网应用创建一个巨大的、可扩展的室外网络。截止到2010年第三季度，该修订方案的工作正处在一个非常早期的发展阶段。

0.2 ZigBee和其他

ZigBee联盟绝大部分都是由撰写IEEE 802.15.4标准最初版本的专家共同创立的。ZigBee联盟的目的是在IEEE 802.15.4标准之上增加通信层，以实现一个完整的协议（按照7层ISO/OSI通信分层模式）以及为它在商业和住宅市场领域的成功提供市场需求。然而，现在很多其他基于通信的协会都将IEEE 802.15.4标准用

在各种应用领域。例如智能对象互联网协议（IPSO）联盟，其推进 IETF 6LoWPAN 协议的使用；HART 通信基金会，推进使用名为 WirelessHART 的工业级的无线通信协议；这本书的第 4 部分详细介绍了 WirelessHART 技术。

这本书的第三版通过增加了以完整描述 WirelessHART 协议为中心的新章节扩充了之前的版本。这是目前为工业传感器网络应用提供的唯一的高可靠性和高性能的国际标准。这种应用类型代表了 IEEE 802.15.4 标准性能要求的最高水平，因为它包括了超低功耗、保证了吞吐量和延迟时间、以及最高的安全等级。同样的，新的章节提供了更多关于 IEEE 802.15.4 标准如何满足这种关键性能要求的详解。

0.3　本书结构

本书是对 IEEE 802.15.4 标准的补充。它概述了 IEEE 802.15.4 标准具有的特征、动机和应用，以及一些关键技术的基本原理。IEEE 802.15.4 标准是以一种让读者容易理解和容易实现的方式来撰写和组织的。IEEE 802.15.4 标准的技术编辑团队特别集中于撰写信息量巨大的章节，从而来阐述本标准中一些复杂的概念。这本书并不打算像标准里一样对一些概念进行阐述（除了应用方面的讨论），而是打算成为该标准的一个指导性书籍。本书针对的是那些对“简单”无线连接感兴趣的人群。本书还主要涉及了工业无线传感器和执行器网络。

本书主要分为 4 个部分。第 1 部分概述了低速无线个域网技术和 IEEE 802.15.4 标准。本部分的内容主要集中于讲解创作本标准的动机，包括驱使完成本标准的应用场景。第 1 部分不仅仅是对标准进行了技术性的介绍，还为市场和商业专业人员提供了足够的背景信息和概念背后的愿景，以帮助他们规划市场和商业策略。

第 2 部分主要阐述了 IEEE 802.15.4 标准的技术特点和组成部分。在网络层功能部分增加了一些 IEEE 802.15.4 标准之外的新内容。这些网络层信息可有助于理解标准中几个关键技术背后的基本原理以及预想的应用领域。第 3 部分重点关注于系统实现和设计方面的考虑。包括对系统级别的现实世界的问题进行分析，而这对于那些未来的实现者来说是很重要的。最后，第 4 部分包括了 WirelessHART 通信标准，详细介绍了如何在 IEEE 802.15.4 标准技术的基础上建造一个高性能和高可靠性的工业标准。

IEEE 802.15.4 标准中的信息是非常简洁的，同时整个标准的上下文也可以反映出其简易性。IEEE 802.15.4 标准分为 7 个章节和 7 个附录。第 1 章～第 5 章包括一些介绍性的内容，对应本书的第 1 部分。标准中的第 6 章和第 7 章分别定义了物理层和媒体访问控制（MAC）子层，这两章对应着本书的第 2 部分。最后，正如之前所解释的一样，本书的第 3 部分和第 4 部分并不与标准相对应，因为这两部分涉及的是实现和使用标准中并不涉及的上层协议。

缩略语和缩写

ACK	Acknowledge	确认
ACL	Access control list	访问控制列表
AES	Advanced encryption standard	高级加密标准
ASK	Amplitude shift - keying	幅移键控
BPSK	Binary phase shift - keying	二进制相移键控
BSP	Beacon synchronization parameter	信标同步参数
CAP	Contention access period	竞争访问周期
CBC - MAC	Cipher block chaining message authentication code	密文分组链接 - 报文鉴别码
CCA	Clear channel assessment	空闲信道评估
CCM	Counter mode + CBC - MAC	计数器模式和密文分组链接 - 报文鉴别码
CFP	Contention - free period	非竞争周期
CRC	Cyclic redundancy check	循环冗余检验
CSMA - CA	Carrier sense multiple access with collision avoidance	带碰撞避免的载波侦听多址访问
CSS	Chirp spread spectrum	线性调频扩频
CTR	Counter mode	计数器模式
CWPAN	Chinese Wireless Personal Area Network	中国无线个域网
DLL	Data link layer	数据链路层
DSSS	Direct sequence spread spectrum	直接序列扩频

DPDU	Data link protocol data unit	数据链路层协议数据单元
ED	Energy detection	能量检测
ETSI	European Telecommunications Standards Institute	欧洲电信标准组织
EVM	Error - vector magnitude	误差矢量幅度
EUI	Extended Unique Identifier	扩展唯一标识符
FCC	Federal Communications Commission	［美国］联邦通信委员会
FCS	Frame check sequence	帧检验序列
FFD	Full function device	全功能设备
FHSS	Frequency hopping spread spectrum	跳频扩频
FM	Frequency modulation	调频
GFSK	Gaussian frequency - shift keying	高斯频移键控
GSM	Global system for mobile communication	全球移动通信系统
GTS	Guaranteed time slot	保障时隙
HART	Highway addressable remote transducer	高速可寻址远程传感器
HCF	HART Communications Foundation	HART 通信基金会
HVAC	Heating, ventilation, and air conditioning	供暖、通风和空调
IC	Integrated circuit	集成电路
IrDA	Infrared data association	红外数据组织
ISM	Industrial, scientific, and medical	工业、科学和医疗
ITU - T	International Telecommunication Union - Telecommunication Services	国际电信联盟远程通信标准化组织
LAN	Local area network	局域网

LBT	Listen before talk	先听后说
LC	Inductor - capacitor	电感 - 电容
LLC	Logical link control	逻辑链路控制
LQI	Link quality indication	链路质量指示
LR - WPAN	Low - rate wireless personal area network	低速率无线个域网
LSB	Least significant bit	最低有效位
M2M	Machine to machine	机器对机器
MAC	Medium access control	媒体访问控制
MCPS - SAP	MAC common part sublayer service access point	MAC 层公共部分子层服务接入点
MFR	MAC footer	MAC 层帧尾
MHR	MAC header	MAC 层帧头
MIC	Message integrity code	消息完整性代码
MIPS	Million instructions per second	每秒处理的百万级的机器语言指令数
MLME	MAC sublayer management entity	MAC 子层管理实体
MLME - SAP	MAC sublayer management entity service access point	MAC 子层管理实体服务访问点
MSB	Most significant bit	最高有效位
MPDU	MAC protocol data unit	MAC 协议数据单元
MPSK	M - ary phase shift - keying	M 进制移相键控
MSDU	MAC service data unit	MAC 服务数据单元
MSK	Minimum shift - keying	最小移频键控
Network Graph	Abstract representation of network addresses in a mesh route	网状路由中一些网络地址的抽象表示
OEM	Original equipment manufacturer	原始设备制造商

O-QPSK	Offset quadrature phase shift-keying	偏值四相移相键控
OSI	Open systems interconnection	开放系统互连
OUI	Organizationally Unique Identifier	组织唯一标识符
PAN	Personal area network	个域网
PD-SAP	PHY layer data service access point	PHY 层数据服务访问点
PDU	Protocol data unit	协议数据单元
PHY	Physical	物理层
PHR	PHY header	物理层帧头
PIB	PAN Information base	个域网信息库
PLME	PHY layer management entity	物理层管理实体
PLME-SAP	PHY layer management entity service access point	物理层管理实体服务访问点
PN	Pseudo-noise	伪随机噪声
POS	Personal operation space	个人操作空间
PPDU	PHY protocol data unit	物理层协议数据单元
PSDU	PHY Service Data Unit	物理层服务数据单元
PSSS	Parallel sequence spread spectrum	并行序列扩频
QoS	Quality of service	服务质量
RAM	Random access memory	随机存储器
RC	Resistor-capacitor	电阻-电容
RF	Radio frequency	射频
RFD	Reduced function device	精简功能设备
RFID	Radio frequency identification	射频识别

RSSI	Received signal strength indication	接收信号强度指示
RX	Receive or receiver	接收或接收机
SAP	Service access point	服务访问点
SAW	Surface acoustic wave	声表面波
SHR	Synchronization header	同步帧头
SNR	Signal - to - noise ratio	信噪比
SoC	System - on - a - chip	片上系统
SSCS	Service specific convergence sublayer	服务特定汇聚子层
TDMA	Time division multiple access	时分多址
TSCH	Time slotted channel hopping	时隙信道跳频
TX	Transmit or transmitter	发送或发送机
VCO	Voltage controlled oscillator	压控振荡器
UWB	Ultra - wide band	超宽带
Wi - Fi	Wireless fidelity	Wi - Fi
WLAN	Wireless local area network	无线局域网
WPAN	Wireless personal area network	无线个域网
WMAN	Wireless Metropolitan Area Network	无线城域网
WSN	Wireless sensor network	无线传感器网络

第1部分

第1章　IEEE 802.15.4标准——让无线传感器网络成为可能

在几乎所有电子设备中存在的嵌入式控制与监测应用，随着其爆炸式的增长，这些应用间相互通信的需求正在引发瓶颈问题。为了解决这个问题，制造商们使用了各种不同的通信接口——标准的或者专有的——创建独有的任务，以此来实现应用间的相互通信。传统的通信链路是通过有线方式实现的，既能为控制器和外围设备供电，还能为两者之间提供可靠的信号传输。但是，当这些外围设备实体不是被包含在控制器里时，有线布线将会带来诸如安装成本、安全以及线缆操作的便利性等问题。无线技术能有效规避这些弊端，但是它同时也面临着很多挑战，例如传播、干扰、信息安全、规则和一些其他的问题。能克服这些问题的无线技术存在，但是随之会增加系统的复杂性，从而导致系统成本的增加。

当然，有些应用能承担得起使用一些高端无线通信系统，例如移动电话中的宽带数据服务、IEEE 802.11™标准的无线局域网、IEEE 802.16™标准无线城域网（WMAN）等。然而，对于很多无法负担得起高端无线通信系统的应用而言，通过采用基于IEEE 802.15.4技术的低成本无线通信解决方案，它们也得以实现或者功能得到加强。标准促进了不同制造商提供的设备之间的互操作，扩大了经济领域，加速了产业成熟，最大限度降低了产品开发者的风险，从而直接让终端消费者从中受益。

基于IEEE 802.15.4标准的低速无线个域网（LR - WPAN）是为机器设备间低成本、超低功耗、短距离无线通信而设计的网络。它与当前无线技术趋势相左，后者致力于发展支持多媒体应用的、高数据吞吐量和增强型服务质量（QoS）的技术。

当前的无线技术趋势是首要考虑更高数据吞吐量和QoS，成本和能耗因素其次。而LR - WPAN的首要衡量标准是成本和能耗，而对数据吞吐量要求比较宽松。

1.1　WLAN、WPAN和LR - WPAN

无线局域网（WLAN）是对IEEE 802®有线局域网（LAN）的无线扩展，是

用于高端的无线数据网络，基本要求包括无缝漫游功能、报文转发功能、尽可能远的传输距离以及允许大量设备接入的能力。不同于 WLAN，无线个域网（WPAN）工作于个人操作空间（POS），覆盖区域为个人周围环境，无论该环境是静态的还是动态的。

WPAN 用于在相对短距离的相关收发器之间传输信息。不同于 WLAN，基于 WPAN 网络的通信很少甚至不需要其他基础网络设施的辅助，这使得在各种各样的设备上都能实现这种体积小、高能效、价格低廉的解决方案。

IEEE 802.15 工作组根据数据率、电池消耗和 QoS 将 WPAN 分为三种类型：

1）高数据率的 WPAN（IEEE 802.15.3™标准），适用于需要很高 QoS 的多媒体应用中。

2）中速 WPAN（IEEE 802.15.1™标准/Bluetooth），被设计用来替代以移动电话和 PDA 为核心的消费电子设备之间的有线连接，其 QoS 需要能满足语音应用。

3）LR－WPAN（IEEE 802.15.4 标准），专门针对低功耗和低成本的应用，而这在前面所提及的两种 WPAN 中是不被支持的。基于 LR－WPAN 的应用对于数据率和 QoS 要求比较宽松。

图 1-1 描述了基于 IEEE 802 标准的 WMAN、WLAN 以及 WPAN 标准的应用范围。值得注意的是 IEEE 802.15.4 标准的应用范围并没有与更高端的无线网络标准的应用范围相重叠。

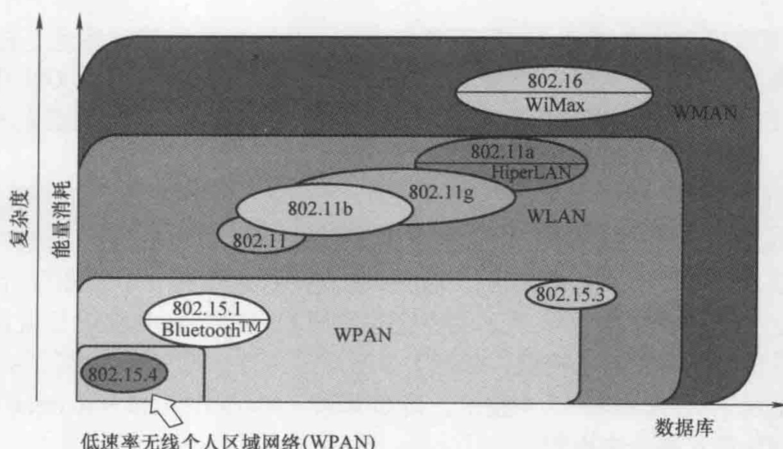


图 1-1 WMAN、WLAN 以及 WPAN 的应用范围

IEEE 802.15.4 标准并非用于与其他无线网络技术竞争，而是在不同的数据率、能量消耗和低成本上完善可用的无线技术。尽管 IEEE 802.15.4 标准也可以用于其他一些应用，但它并不是设计用于将它和其他无线网络标准的应用范围进行重叠的。作者十分不赞成将 IEEE 802.15.4 标准用于传统的 WLAN 应用，这样做可能是十分充满挑战的尝试（有着非常大的传输延迟）。

表 1-1 显示了使用 IEEE 802.15.4 标准的 LR－WPAN 的一些重要特性，并将 IEEE 802.11b/g 与一个标准的 WPAN（如 IEEE 802.15.1™标准）相比较。

表 1-1　802.15.4LR－WPAN 与其他无线技术的比较

	802.11b WLAN	Bluetooth™ WPAN	802.15.4 Low Rate WPAN
室内距离	1～30m	1～30m	1～30m
数据吞吐量	2～11Mbit/s	1～2Mbit/s	≤0.25Mbit/s
功耗	中	低	最低
尺寸大小	大	较小	最小
复杂性	>6	1	0.2

LR－WPAN 致力于一些采用其他 WPAN 方案仍旧十分昂贵的应用，要求极低功耗的应用，和/或某种技术（例如蓝牙）的性能无法满足要求的应用等。

LR－WPAN 完善了无线网络技术，它在极低实现成本的情况下提供了非常低功耗的能力，这使得之前无法实现或者需要采用专有技术的应用成为可能。

1.2　ISO/OSI 参考模型

IEEE 802 通信标准仅定义国际标准组织（ISO）公布的开放系统互连（OSI）协议参考模型中最底的两层：即物理层（PHY）和数据链路层[19]。OSI 模型中的其他层在 IEEE 802 通信标准中没有被规定，一些对标准感兴趣的制造商和用户联合组建了工业联合会，并对这些层进行了明确定义。

层次化的参考模型允许将各层中明确定义的功能进行不同等级的抽象和组合。参考模型中的每层通过服务原语给上层提供服务。

对于 IEEE 802.15.4 标准而言，ZigBee 联盟就是这样的一个工业联合会组织。它通过制定应用行规文件引导了上层协议的发展和完善。这些应用行规使用了一个简化的五层 ISO/OSI 参考模型，如图 1-2 所示。另外，近年来一些其他的无线通信标准也使用了 IEEE 802.15.4 技术，诸如 IETF、6LoWPAN 和 WirelessHART，这些会在本书的第 4 部分中讲到。

ZigBee 联盟是由一些业内领军的制造商、经销商和终端用户组建而成的联合会，致力于发展住宅和商业应用的规范，包括家居和楼宇自动化、商业和零售业监控与管理、健康护理等。

HART 通信基金会（HCF）是由工业过程控制领域的领军企业组成的组织，负责包括 WirelessHART 在内的 HART 标准的管理和控制，主要专注于工业仪表领域。这些标准组织已经制定了一些包括网络支持和应用规范的上层协议，从而与 IEEE 802.15.4 射频技术相结合成为一个完整的通信协议。

ISO/OSI七层协议模型	简化的ISO/OSI五层协议模型	IEEE 802标准协议模型
7 应用层	用户应用层	上层
6 表示层	应用行规	
5 会话层		
4 传输层		
3 网络层	网络层	
2 数据链路层	数据链路层	逻辑链路控制子层(LLC)
		媒体访问控制子层(MAC)
1 物理层	物理层	物理层(PHY)

图 1-2 ISO/OSI 参考模型及 IEEE 802 标准模型

1.3 无线传感器网络

无线传感器网络是无线网络应用的一个分支，用于在没有有线连接的情况下为传感器和驱动器之间建立连接。

传感器网络可以根据传感器类型、应用领域（工业、医学、汽车等）、工作环境（爆炸、振动、加速度、温度等）以及网络参数（网络拓扑、需求吞吐量、传播距离等）进行分类。IEEE 802.15.4 工作组把应用领域重点放在无线传感器网络上。

由于“Wireless Sensor and Actuator Networks（无线传感器和执行器网络）”的名字长度过长，工业界采用“Wireless Sensor Networks（无线传感器网络）”代替。这种类型的网络用于收集和发送信息到无线收发器，这些无线收发器连接着一个传感器和/或一个驱动器。

人们之所以对无线传感器网络感兴趣源于三个方面的原因。

第一、更低的传感器安装成本。传统的传感器安装成本来自布线、人力成本、材料、测试以及验证。例如，一个限位开关可能花不到 1 美元，而设备的安装成本可能多达 50 ~ 100 美元。类似的，一个工业压力传感器可能花几百美元，但是将它

和中心控制器通过线缆连接起来的成本可能高达 300 美元/ft（1ft = 0.3048m）。此外，在工业和住宅环境下进行的规范布线需要额外的材料和安装作业，例如电缆管和受过专业培训的安装劳力。

第二、有线连接方式存在缺陷，它需要很多连接件，而这些连接件可能由于振动、环境因素、频繁接入相邻设备而变松、丢失、接触不良或者受损。这个问题被称为“最后一米连接问题”，它因与广域网“最后一公里连接问题”相似而得名。

第三、无线传感器网络形成了更底层的智能维护系统，使得在传感器密集的环境下能够获取大量可被用于改进工业流程的数据。同时，无线传感器网络能以更高的频率采集机械设备和工业系统的数据。相比较而言，通过硬线将传感网络和中心系统连接起来的有线网络大大增加了系统的复杂性，因而在大多数情况下并不实用。

传感器网络的无线解决方案提供了更灵活的连接方式而无须连接件。除此之外，使用无线系统还使工业作业更加安全。例如，过去需要在危险环境下进行的人工作业可以由无线监测点代替。当然，无线传感器网络也如其他无线应用一样存在着一些问题，如信息安全、身份验证、小范围的射频传播、天线放置问题等。

可移动性是无线解决方案的另一个优点，而在无线传感器网络定义中这种能力被解释为“易安装”。尽管可移动性并非无线传感器网络系统的主要需求，但是某些移动性的概念可用于实现自组织（Ad Hoc）网络。需要注意的是，本文中提到的可移动性指的是设备间的相对运动。例如，在一个运动的机器中，如果其内部的传感器只和这台机器内部设备通信，那么这些传感器组成的无线传感器网络不能认为是动态的。

上面所描述的一系列无线通信系统的优点并不足以完全取代有线连接方式。有线网络的可靠性和安全性（感觉上的和实际情况）仍高于无线通信系统。可以预见，有线和无线网络的混合网络将会出现，有线和无线网络将会共存并且互相弥补不足。那时，无线传感器网络将作为有线网络的拓展，被应用到某些特定的应用上。

1.3.1　无线传感器网络设计中面临的挑战

到目前为止，无线传感器网络（WSN）技术的应用仍发展缓慢，根本原因在于缺乏能使开发者们专注于应用层面和通信方面的标准化技术。无线产业界当前的发展重点放在了更高数据吞吐量的无线通信，而遗忘了短距离连接的需求。

对 WSN 来说，一方面需要具有易于安装大量收发器的能力；另一方面面临着无线通信存在的众多问题（如传播距离），以及来自具体应用中独特的挑战，例如将一些特殊设备（如一盏台灯和它的开关）进行逻辑绑定的需求。

在此情况下，所有可能实现 WSN 的技术有：

1）光通信：这个技术包括红外数据通信（IrDA®）标准等。这个技术的主要缺点是在这种类型网络中的设备需要工作于一个无障碍的视距范围内。

2）场感应：这种技术已经被广泛应用于无线射频识别（RFID）应用，其主要缺点是非常短的传输距离和需要高能量的网络协调器。另外，高效的通信还需要进行电场校准。

3）超声波：和场感应技术相似，超声波技术也需要高能量的网络协调器。其主要的问题不再是视距通信，而是传感器体形要素（小型化趋势）。

4）电力线载波通信：这种技术是将数据信号叠加到电力线上。近年来，它已经发展成熟，可以广泛用于以家庭网络为主的一系列应用中。值得注意的是，该技术由于没有使用更多新的电缆而被认为是无线技术。

5）射频（RF）：该技术不需要通信区域在无障碍视距内。目前该技术已经实现了数据率和传输距离可根据应用需求而调整的低功耗无线电收发器。

射频技术似乎在无线传感器网络实现上拥有很大的优势，但是它也存在很多问题有待解决。下面章节介绍了在无线传感器网络的设计和实现过程中遇到的一些重要问题。

1.3.2　功耗问题

一些应用需要使用到完全不受限的射频收发器（不接入外部电源），这意味着需要使用电池供电或者使用电能收集技术。如果采用电池供电，由于功耗问题，电池不得不频繁更换，使得传感节点维护成本增加，与易安装、低成本运行的初衷是相违背的，那么就要求电池必须能持续使用很长时间。另外，电源受限的另一个直接影响就是通信距离也受到了限制。

针对这个问题，一种常用的解决办法就是实行功率循环，即降低设备的运行占空比。这种方法又引出一个网络同步问题，而该问题也可通过采用合适的网络技术来解决。

通过简单计算可以知道，让一节容量为 750mA · h 的 AAA 电池为一个现有的短距离无线电收发器（活跃期典型电流消耗为 10mA）供电，如果这个收发器占空比小于 0.2%，那么其供电时间可超过五年。

一般而言，无线传感器网络不会使用充电电池，这种充电电池通常用于如手机和 PDA 等消费类电子产品。

1.3.3　传输距离问题

在免牌照频段，由于政府相关规定和从经济上考虑，无线系统工作的典型 RF 功率输出为 0 ~ 20dBm（1 ~ 100mW）。受限的功率导致受限的连接距离——即一对接收机和发射机最远传输距离是受制约的。在 WSN 环境中，多跳网络协议通过选取合适的路由算法可以避免这个限制。

同其他无线网络无线电技术相比，基于IEEE 802.15.4的设计能使其无线电收发机工作在极低的功耗水平。如果RF的输出功率为0dBm，无线电收发器灵敏度为-70dBm，那么在一般室内环境（使用指数为3的路径损耗模型）下其通信距离为10m（30ft）。目前一般无线电收发器灵敏度达到-90dBm或者更高，其室外通信距离超过了100m。

1.3.4 可用频带

无线电频谱是一种稀有资源，其使用规则由政府制定。但是，有一些特别的免牌照频带，只要无线设备的射频输出信号满足时间、频率和振幅上的一些要求，无线设备就可以在该频段使用。对于某些频带，在一些规定区域，为了实现更大的射频输出功率，必须进行能量扩展，例如使用扩频调制。由于免牌照频带的使用是免费的，于是制造商们只需遵守频带使用规则即可。

对于无线传感器网络，以下是常用频带（或者计划使用）：

1）868.0~868.6MHz：在大部分欧洲国家可用。

2）902~928MHz：在北美可用。

3）2.40~2.48GHz：在世界上大多数国家可用。

4）5.7~5.89GHz：在世界上大多数国家可用。

工作于免牌照频带的无线电设备必须遵守当地规则。在美国，联邦通信委员会（FCC）是管理这些无线电设备的机构。同样的，在欧洲，欧洲电信标准协会（ETSI）努力协同监管。世界上其他国家都有自己的监管机构，它们中的许多或采用FCC标准或采用ETSI标准作为本国的准入标准。

IEEE 802.15.4包含有一个资料性的附录，它重点关注了世界各地的频带管理需求。尽管该资料只是入门级的，但它可为开发者提供足够的背景信息，使他们开始为完善制定频带使用规则而努力。

工作于全球免牌照频带的无线网络标准提供了潜在的更低成本的解决方案，而通过技术进步、扩大生产和减少重复设计（无须重新修改）使得成本得到降低。近年来，由于在2.4GHz和5.7GHz频段有大量可用带宽，一直专注于短距离无线通信的原始设备制造商（OEM）也开始进军这些频段。

现在，人们已经普遍意识到了无线通信标准共存这一问题。当互不相容的几种技术共享同一频段时，在获取频带和接入过程中就会引发冲突。一些研究评估了这个问题的影响，研究表明这些潜在的冲突问题与通信负荷、空间分布、射频输出功率、收发密度、射频信道以及射频传播参数有关。

原始的 IEEE 802.15.4 设计工作于以下频段：

1）868.0～868.6MHz：1 个信道（20kbit/s、100kbit/s、250kbit/s）。

2）902～928MHz：10 个信道（40kbit/s、250kbit/s）。

3）2.40～2.48GHz：16 个信道（250kbit/s）。

前两个频段统称为“低频段”，第三个被称为“高频段”。最新版的 IEEE 802.15.4™标准（例如 IEEE 802.15.4c/d）在定义其他频段或者使用不同调制方式的已有频段时（如 IEEE 802.15.4a），仍然使用这种分类方法。

1.3.5 网络拓扑

通过建立一个网格状拓扑结构的多跳网络可以克服单个收发器有限的传输距离。无线传感器网络的一个要求就是低维护成本。为了达到这个目的，网络拓扑需要被设计成允许网络中的设备工作于低占空比。第 6 章分析了适合无线传感器网络的网络拓扑和网络层。

一直以来，有一个容易被忽视的重要事实：无线网络意味着网络中设备之间能双向通信。这个特性增加了系统的可靠性，并且使得监测所有设备的状态成为了可能。

1.3.6 自组织

为了易于安装，无线网络必须能实现自组织，也就是说，每个传感设备无须特别的现场配置（如地址分配、关联和通信量均衡）就能加入网络。

自组织是 Ad Hoc 网络的一个特征。Ad Hoc 无线网络是由一大批收发器组成的网络，而无须任何固定设施或者集中管理系统的辅助。该网络根据路由协议选择合适的从源设备到目标设备的消息路径。例如，在某种协议中，每个无线电设备存储一个与邻居无线电设备的连接列表，并且在网络拓扑结构发生改变时更新路由表。

自组织策略是网络拓扑、网络安全和应用需求的聚合体，它通常基于应用行规的相关定义来实现。应用行规并非 IEEE 802.15.4 标准的一部分，它将具有相同功能的应用统一起来，从而实现遵循标准的设备之间的互操作。

第2章　低速无线个域网的应用——愿景激励

IEEE 802.15.4 标准应用广泛，主要适用于低功耗、短距离、数据吞吐量要求不严格的简单无线传输应用场景。IEEE 802.15.4 标准的应用可归类如下：

1）可粘贴传感器：这一类应用涉及完全无须线缆连接的无线传感器，其中包含有电池供电的收发器。这类应用主要集中于监控或远程诊断。

2）虚拟线缆：在线缆连接布置困难时，某些监测和控制应用就只能依靠无线通信连接。例如轮胎压力监测、电动机轴承及发动机部件故障诊断等应用场景。

3）无线集线器：在某些实际应用中，集中式无线网桥需要加入到有线网络中去。无线集线器在有线网络和无线 LR-WPAN 网络中间起着网关的作用。在许多情况下，无线集线器网络由两个收发器组成，一个为集线器，另一个为嵌入其他设备（例如嵌入 PDA 设备）中的 LR-WPAN 设备。

4）替代线缆：这类应用通过移除无线传感器设备中的通信线缆来增加其应用的价值。其中，某些应用已采用另一种 WPAN 技术：IEEE 802.15.1（蓝牙）标准。在这种情况下，IEEE 802.15.4 标准提供了另一种低功耗的方案（功耗至少降低一个数量级），并且随着功耗的降低，带来了其他好处。替代电缆不同于“可粘贴”传感器应用，因为前者可能采用某种可持续的电源（如有线电源）或者是可更换的电池。

图 2-1 显示了上文中提到的 LR-WPAN 具体应用场景。

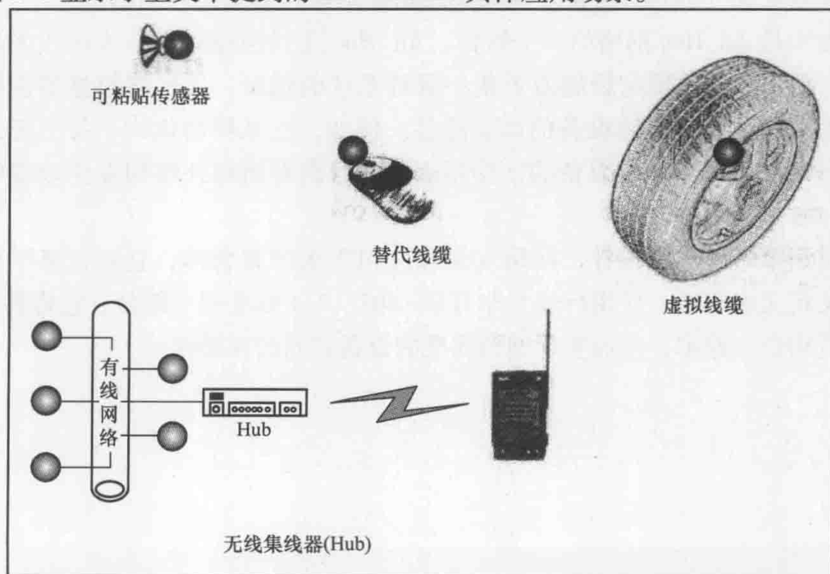


图 2-1　LR-WPAN 应用场景示例

应当指出，对IEEE 802.15.4标准的关注是为了将其更好地应用于具体应用中，标准的价值体现在应用中，而不是体现在无线性能上。这种意愿可能会与其他更注重通信性能的应用相冲突，例如移动通信应用。

本章讨论了一些基于IEEE 802.15.4标准的具体应用，这些应用是由许多领军企业和有远见的专家提出的，并且激励着IEEE 802.15.4标准的制定。

IEEE 802.11、IEEE 802.15.1、IEEE 802.15.3标准是针对特定应用提出的，而IEEE 802.15.4标准却适用于不同市场中的多种应用，始终着眼于无线传感器网络中的通信。

2.1 工业和商业控制与监测——无线传感器

正如第1章中提到的，在工业及商业领域，无线连接主要用于降低传感器及执行器的安装成本，同时构建传感丰富的环境，作为智能嵌入式系统的底层应用。

基于IEEE 802.15.4标准的应用，通常是监测应用。这类应用中传输的数据为非关键性数据，并且允许较长的时间延迟。一般说来，此类工业监测应用也不需要很高的数据吞吐量或者持续数据更新。相反，此类应用更注重降低设备的功耗，以尽可能地延长网络设备的电池使用寿命。过程控制应用却是个例外，虽然不要求较高数据吞吐量，但是控制时延和总体可靠性是此类应用中必须考虑的问题。正如第4部分中描述的，IEEE 802.15.4标准技术可以保证此类应用必要的可靠性。

工业自动化中的典型应用包括无线接入点，该设备可作为有线工业协议（例如HART®、Field - bus®、PROFIBUS®及其他）的网关。通过这些无线接入点，可以监测经由PDA（无线集线器）连接到有线网络中的设备，并且配置其参数；也可以建立起与某个网络设备之间的无线连接（取代电缆）。图2-2为上文提到的典型工业用例示意图。

HART通信基金会是一个行业组织，针对过程控制应用的特定情况而组建，支持并促进基于IEEE 802.15.4标准的WirelessHART标准。WirelessHART标准在国际上又被称为IEC62591。

一般而言，工业应用没有某种特定的网络拓扑。IEEE 802.15.4网络固有的拓扑灵活性，使其广泛适用于不同工业设备应用中。

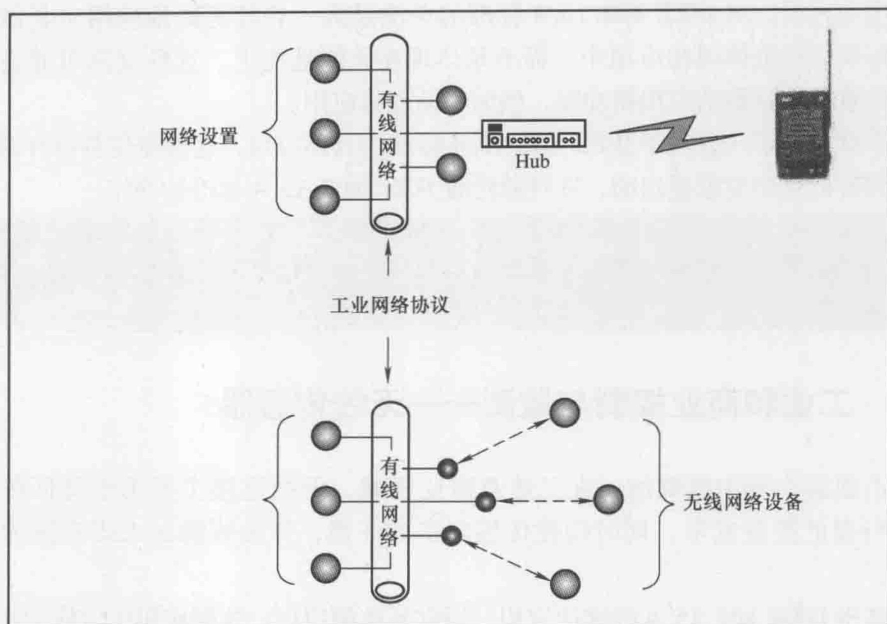


图 2-2　典型工业用例

2.2 住宅智能能源

到 2050 年，全球能源消耗预计增长 2 ~ 3 倍，在有关能量可持续利用的讨论中，生产和消费两端的能量管理将占有越来越重要的地位。“智能电网”代表着一种理念，涉及电力传输和配电网络的数字化升级，能够更好地进行峰值消耗管理，集成分布式替代能源的生产，用户也能够更好地控制能量使用。

最初的设想是，电网峰值管理由公用电力公司电力需求响应过程触发，或者由大型用户应用的远程启动，例如供暖、通风和空调（HVAC）系统、插入式混合动力等来触发。另一种电网峰值管理的策略基于动态电价，电力公司将价格信息发送给用户用电设备，引导他们在电价较低的时间段内使用高电能消耗的设备（假设在此时间段内，系统有承担这种高电能消耗载荷的额外能力）。

过去，从用户角度来看，实现智能电网愿景遇到的最大挑战来自于住宅市场领域。家庭住宅通常缺少标准的通信设施，不能有效地协调并管理电力载荷的需求响应和动态价格。然而，随着基于 IEEE 802.15.4 标准网络的应用，上述问题将得到缓和。基于 IEEE 802.15.4 标准的廉价房域网（Home Area Network，HAN），只需对住宅环境做简单改造，就能实现对家用电器的监控以及对能量消耗的管理控制功能（可由电力公司远程管控，也可由用户本地控制）。

基于 IEEE 802.15.4 标准的 ZigBee 协议于近期提出了一套应用行规。其中，某个行规可被用于创建特定类型的房域网，包含能量监测和控制功能，该行规被称为"智能能源行规"。

2009 年，美国政府将 ZigBee 智能能源行规作为房域网与智能电网之间的无线通信接口标准。

2.3 家居自动化与网络化

用户与家居自动化市场由于其规模巨大，具有极高的市场潜力。基于 IEEE 802.15.4 标准的 LR－WPAN 设备可以以极低的成本取代家居环境中的家用线缆。潜在的无线传感设备包括消费电子产品、个人电脑外围设备、交互式玩具与游戏，以及家居安全、照明控制和空调系统等[2]。上述应用中的大多数受到有兴趣采用低功耗无线解决方案的工业团体的关注。这些工业团体包括：消费电子协会（Consumer Electronics Association，CEA）、家庭插座联盟、ZigBee 联盟。特别有意思的是，ZigBee 联盟提供的分析报告将 LR－WPAN 在家居自动化的应用定义为：较低的数据吞吐量、可接受的较高的报文传输时延。

经过对家居自动化应用性能的分析，IEEE 802.15.4 标准的最大传输速率设计为 250kbit/s。

2.3.1 消费电子产品

消费电子产品包含收音机、电视机、VCR、CD 播放器、DVD 播放器、远程控制设备以及其他通常意义上的家电设备。将产品和服务与常见控制机制（基于 IEEE 802.15.4 的远程控制）结合成整体，这带来了许多有趣的机遇。随着个人电脑市场与消费电子市场的结合，遵循 IEEE 802.15.4 标准的终端用户就可以从两端控制设备，而使用的就是他们熟悉的直观设备——远程控制设备。现在，除了减少家庭中远程控制单元的数量之外，远程控制单元也可以由个人掌控，而不再是由设备支配。个性化和双向远程控制已经成为可能，这也丰富了编程和控制功能。此外，在基于 IEEE 802.15.4 标准建立的常见通信基础设施支持下，用来控制家庭娱乐中心音量、音频均衡器及其他设置功能的多媒体间通信连接即将实现，自动调温和具有安全功能的家庭系统也即将成为现实。

2008 年 6 月，为制定消费电子产品的远程控制标准，RF4CE 联盟应运而生，其服务对象为基于 IEEE 802.15.4 标准的消费电子产品。该联盟的目标是在五年之内取代红外远程控制技术，使用更快、更稳定的非视距技术来操作消费电子产品。此外，IEEE 802.15.4 标准具有的双向通信能力，可实现设备与远程控制器之间更为高级的通信，提供更好的用户体验。

2009 年 3 月，RF4CE 联盟与 ZigBee 联盟合并，以针对基于射频控制的家庭娱乐产品开发出新的标准规范，完善 ZigBee 的愿景。

2.3.2 个人计算机外围设备

计算机外围设备包含无线鼠标、键盘、操作杆、PDA 和游戏，代表了可实现低速无线连接的大部分家用设备。此外，PC 制造商和软件公司试图改进 PC 设备的接口，使其更加面向用户。远程控制和 PDA 将变成新的 PC 控制方式。IEEE 802.15.4 技术将为此类应用场景提供独特的低功耗、低成本解决方案。

2.3.3 家居自动化

家居自动化，包含供暖、通风、空调（HVAC）设备、安全、照明，以及对诸如窗帘、窗户、门、锁等设施的控制，代表了家庭内部无线创新技术应用的好机会。温度调节器通常被放置在房屋中很少有人长时间逗留的区域，例如走廊、门厅等区域。这将导致温度调节器测得的温度与人在室内感知的温度不一致，正因如此，对室内环境的控制效率通常不高。

无线温度调节器可以分散地分布于整个房屋内，与 HVAC 系统中的无线通风控制器（分区控制器）连接，独立地调节各个房间温度。白天，电视打开时，窗帘会自动拉合；壁挂钟与主基准时钟协调，这样其在重启后能自动调校时间。无线烟雾检测器和玻璃破碎探测器连接到家居安全系统中，而家居安全系统的操作可以像汽车远程遥控钥匙一样简单，按下一个按键就可以锁上所有的门窗。在基于 IEEE 802.15.4 标准的应用支持下，常见的远程控制可用于实现上述控制功能，并且实现对家用电器的控制。

某些照明制造商最近宣称，已经将基于 IEEE 802.15.4 标准的无线收发器集成到灯泡和镇流器上。使用这种照明设备，不用架设电线（在家庭重装修中非常实用），标准的无线开关可以安装在室内任意位置，而且不用担心穿墙带来的麻烦。

2009 年 11 月，ClimateTalk 联盟成立。该组织致力于基于 ZigBee 智能能源行规来定义通用信息模型，同时还致力于标准化 HVAC 信息系统。

2.3.4 家居安全

与家居自动化类似，安全传感器也分散在家居环境中。典型安全传感器包含运动感应器、门窗开关感应器、漏水传感器以及其他专用设备。同样地，使用 LR－WPAN 网络收发器的无线传感器与其对应的有线传感器相比，价值体现在其安装的简易性，即无线传感器的安装不需要考虑布线格局及在墙壁门窗上钻洞等线路架设问题。

无线传感器在家居安全中的应用面临以下两大挑战：

（1）能量的消耗问题。通常，由于这些传感器被安装在门或窗上，因此不适

合采用有线供电。正如前文所述，IEEE 802.15.4 标准采用简单却高效的协议栈结构，能够很好地解决此问题。此外，IEEE 802.15.4 标准的媒体访问控制层（MAC）为上层应用提供了访问接口，通过该接口，上层应用可以完全控制使能或禁用底层射频功能。

（2）射频信号的无线发射距离。IEEE 802.15.4 标准中规定的输出功率通常受两方面因素限制：政府规定和必要的节能。IEEE 802.15.4 标准提供的点对点传输协议，允许附加的网络层（IEEE 802.15.4 标准不包含网络层）实现多跳，从而增加射频信号的有效传输距离。

2.3.5　个人健康护理

个人健康护理包括传感器、监测器和诊断。本部分与医疗遥测是相互独立的两部分，个人健康护理包含慢跑者及其他运动员经常使用到的计步器和心率监测仪等设备。这些设备采集到的数据，通常要传送到显示设备上显示，而无线连接通常是唯一可行的方式。健康记录维护是另一应用，用户的日常体重、体温及其他信息可以通过无线连接方式，在合适的测量设备（如体重计、体温计）之间传输，并存储到个人电脑或 PDA 上。当这些数据信息被共享到互联网上，健康护理专家就可以通过远程访问数据来监控个人健康状况，用户本人也就无须每周去减肥中心了。

近年来，IEEE 802.15.4 技术成为老年人健康护理应用中的关键支撑技术。针对老年人健康护理的应用，通过远程监控独自生活的老年人日常行为状况，来评估其健康状况。通过该应用服务，老年人可以安心地居住在舒适的家中，当其健康状况出现问题时，健康护理专家能够收到报警信号，而远在外地的亲人也可以远程查看他们的近况。在该应用所使用到的众多传感器中，最为人们所熟知的是无线紧急按钮，当老年人身体突发状况时，可通过它发送紧急信号。

ZigBee 联盟定义了健康护理应用行规，旨在通过在设备之间和应用服务之间广泛的使用无线通信技术，为伤残人士和老年人营造安全、健康和独立的生活环境。

2.3.6　玩具和游戏

低速无线网络可为玩具和游戏领域提供很多支持，尤其是玩具之间或玩具与 PC 之间的通信。玩具产品对成本极为敏感，玩具设计过程中遇到的困难，通常不是语言识别和合成等大运算量任务的技术实现问题，而是如何以最低的硬件成本代价实现这些功能。在玩具与其附近的 PC 之间添加无线连接，可以有效地降低玩具成本，因为玩具只需具有无线连接、必需的传感器和执行器（例如扩音器和话筒）即可。这种依靠 PC 的玩具具有复杂的行为能力，而且其行为能力只受限于计算机的运算能力和无线技术的通信能力。该应用领域中还包括个体间或团队间的

无线游戏。除了游戏玩家之间的简单无线连接之外，当玩具和游戏在计算机通信范围内时可接收到更新；即使玩具和游戏离开计算机的通信控制范围，它们也可自动地以新模式、新人物角色或新特性运行。无线游戏制造商使用基于 IEEE 802.15.4 标准的解决方案，可将已有游戏与新游戏连接，因为需要添加的无线模块成本不高、能耗较低，从经济层面上足以吸引用户将其添加到现有游戏中去。

表 2-1 汇总了家居自动化和家庭网络的应用需求。请注意，每个领域中的大多数应用，其典型数据传输速率都远低于标准中规定的无线传输速率的最大值。

表 2-1　家居自动化和家庭网络的应用需求

分　类	要求的最大数据速率/(kbit/s)	最大可接受的报文延迟/ms
消费电子产品	3	16.7
个人计算机外围设备	115.2	16.7
家庭自动化	10	100
个人健康护理	10	30
玩具和游戏	115.2	16.7 ~ 100

2.4　汽车传感

随着汽车的舒适性及功能不断增强，无线通信技术逐步进军汽车行业。第一波无线技术在汽车行业中的应用，最先体现在遥控车门开关及其衍生产品上。第二波无线技术应用高潮，随着车载应用中无线技术“取代电缆”而到来。IEEE 802.15.1 标准/蓝牙技术率先应用于此类应用，广泛应用于电话系统中，例如将移动电话嵌入到汽车中，实现车载免提电话语音系统，以及通过移动电话向汽车传输数据以实现汽车的个性化配置。

不是用来提高汽车安全性能或奢华程度的应用，一般而言都要受到成本的约束。现如今，车身各处分布着众多传感器和执行器，不断增加汽车生产中线缆的需求量，因而也不可避免地影响着汽车安装、诊断、维护的成本，甚至会影响燃料的消耗。

无线技术为传感器和执行器的安装带来了更大的灵活性，使更高级的无线连接取代有线连接成为可能。无线技术在汽车应用中遇到的挑战，来自于如何在相对严酷的汽车环境下满足应用的低功耗需求。

轮胎压力监控系统是无线技术在汽车应用中的一个典型实例。该系统由分别安装在四个轮胎上的四个压力传感器，以及用于接收采集到的数据的中心站组成。压力传感器要分别安装在四个轮胎上，因此不能使用线缆传输数据信号或为传感器供电。因此，传感器需要电池供电。然而，在轮胎更换周期中间，专门去更换传感器或供电电池的想法是不切实际的，因此，供电电池一般要求至少能够正常

工作三年，理想的状况下能够工作五年。对供电电池工作年限的要求，很大程度上限制了电子元件的能耗，并且要求系统有良好的能耗管理能力。大部分情况下，传输数据（测量的压力数据）的大小只有几位，在没有警报的前提下，信息采集的频率大约是每 1 ~ 10min 传输一次。在没有压力骤降的情况下，一般不用担心信息的传输延时。一旦出现轮胎压力骤降情况，中心站将会第一时间得到通知，此时可以不去考虑功耗问题，因为此时一般要对轮胎进行更换。严酷的汽车环境和汽车本身的金属结构，增加了 RF 射频的设计难度。不过双向通信技术的应用，大大增加了通信的可靠性。

2.5 精细农业

LR - WPAN 网络的另一应用领域为精细农业，也被称为精细耕种。精细农业是一个环境友好型系统，在节约耕种成本，减少人类劳动干预，以及由于自然环境的不确定性带来的变化的同时，最大化农业产品的产量和质量。现如今，人类劳动和自然环境仍然在农业中起着重要作用。农耕仍然是以工具为主的，人们通过手工或现场非智能机器进行劳作，这样生产出的农产品数量和质量是无法预知的。采用精细农业新模式之后，耕种将变得更新信息化和软件化，更多地使用基于远程控制的联网自动化智能设备。精细农业需要大规模网状网络支持，可能会有数以千计的传感器通过 LR - WPAN 网络设备连接到网络上。设备上的传感器将采集土壤信息，例如土壤中水分含量、氮浓度以及土壤酸碱度 PH 值。气象传感器采集降雨量、温度、湿度、气压值等有价值信息，也将传送给农户参考。传感器依次将采集到的信息传送给与之通信的 LR - WPAN 网络设备，LR - WPAN 网络设备进而将数据依次传输到中央数据收集设备上。为使传感器数据真实有效，通常要使用定位技术，将每个传感器与其在田地中的位置一一对应起来。各种传感器传输的综合信息，能够针对潜在问题提前向农户发出预警，指导农户生产，这样就能获得更高的粮食产量。精细农业应用位于 LR - WPAN 应用领域的边缘，部署在田地中的传感器每天只需要传输少量几位数据信息。数据流是异步的，而且对时间延迟的要求限制很低。正是基于上述因素，传感器供电电池的寿命通常很长。精细农业网络采用网状网络拓扑结构，某些设备作为其他设备的中继器而为它们转发数据至终点。此外，精细农业网络应当是可自配置的，因为手工配置这种规模的网络通常是不可行的。

2.6 其他应用

消费者市场中出现的一种独特应用是教室计算网络。教师工作站或 PAN 网络协调器，向每个学生的绘图计算机或网络设备上发送任务及数学题目。计算完成

后，学生将其计算结果上传至教师工作站。这种网络只需要支持少量设备节点，并且不支持设备节点间的点对点通信，以免学生互相交换解题方法。此类应用载荷量约为100~500个字节的数据信息，每个学生每小时发送几次。为计算和通信功能提供能量支持的电池，其生命周期应当能够持续一个学期。

无线集线器的另一项重要应用是远程测量和远程配置。此类应用可以为危险操作提供保护，并且能使操作更加便捷。设备通过安装基于IEEE 802.15.4标准的LR-WPAN装置，可与PDA交换数据。该PDA中可以包含预编程的配置信息，或者包含能将数据与大型数据库同步的软件。

第2部分

第3章　IEEE 802.15.4标准技术概述——热身

IEEE 802.15.4标准工作组致力于在固定、便携及移动的廉价设备之间实现低复杂度、低成本且功耗极低的无线连接。在数据吞吐量和数据传输时延要求不高的情况下，低成本、低功耗的设计是可以实现的。随处可见的自由短距离通信的梦想也开始逐渐变为现实。

无线产品的成本主要与管理、销售、市场活动相关，还与无线产品的制造和运行费用有关。为了控制无线产品的总体成本，同时降低设备功耗以延长供电电池寿命，IEEE 802.15.4标准在多个性能指标上做出合理的权衡。符合IEEE 802.15.4标准的设备，使用免执照的射频波段，以减少项目实施方和用户双方的管理成本。符合IEEE 802.15.4标准的服务不需要基础设施支持，通常覆盖范围较小；同时也支持大规模的网络，这样发射和接收能耗极低而且运行成本也要很小。本章列举了IEEE 802.15.4标准中能够满足上述性能要求的一些独有特性。

3.1　低功耗和长电池工作周期的实现

3.1.1　占空比

电池是无线收发系统中成本相对较高的元器件。电池为通信提供能量，其运行与更换同时也是一笔不小的开支。如果系统运行需要价格昂贵的特种电池，那么系统的总体成本不可能很低。而价格低廉的电池，又将限制系统中其他特性的实现。例如，大多数电池在完全充电后，其电容量与瞬时功率传输能力是相关联的。只有限制电池的瞬时功率传输能力，才能充分实现其完全充电后的电容量。正是由于这种限制，电池能量要以极低的速率或者以较低的占空比输出，才能实现电池寿命的最大化。实际无线射频电路的功耗通常是很高的，在恒定运行状态下，电池不可能持续到预期的生命周期。正因如此，符合IEEE 802.15.4标准的设备能够以很低的占空比运行，即设备中的接收器和发射器能够在99%的总运行时间内都处于非活跃状态。

在实际系统中，当无线电路处于非活跃状态时，定时器等元器件仍然会消耗少量的电量，此时的电能消耗被称为待机时的能耗。为减少整个系统的平均功耗，应当尽力

减少活跃时的能耗和待机时的能耗。然而，对于某个特定的技术和一些无线网络支持的应用，活跃时的能耗和待机时的能耗都存在实际的限制。此外，在大多数应用中，活跃时的能耗远大于待机时的能耗。因此，通过降低占空比能够有效地延长电池寿命。

例如，设备活跃时的能耗为10mW，待机时的能耗为10μW；如果占空比为0.1%，则平均功耗为19.99μW。如果设备使用750mA·h的AAA电池供电，电压线性调节为1V，电池可使用37000h，即电池可用4年多。

为能在低占空比条件下正常工作，IEEE 802.15.4标准定义的信标帧在2.4GHz频段上的发送周期为544μs，而超帧周期（网络信标帧之间的时间间隔）可由15.36ms扩展到4min。即信标帧的占空比可设置为2.3%～0.000216%（2.16×10^{-6}）。此外，IEEE 802.15.4标准还支持无信标帧网络。在无信标帧模式下，主从星形网络中的从设备，可无限期地工作于待机模式，只有当有事件发生时才与主设备通信。主设备可能是有线电源直接供电的，因此可以具有连续接收数据报的能力。因此，从设备的电池使用寿命差不多可以是无限长，其主要受限于从设备待机模式时的能耗。无信标帧工作模式，能够很好地满足工作在868MHz频段时的设备性能要求，因为该频段时的最大占空比为1%。

3.1.2 调制

为实现低成本、低功耗的要求，IEEE 802.15.4标准只支持数字通信，不支持模拟通信业务。由于只支持数字通信服务，选取的调制方案通常要求高效且实施成本低。同时，IEEE 802.15.4通信协议支持半双工通信，这样发射器和接收器就不需要同时处于激活状态。

IEEE 802.15.4的物理层采用了一种扩频序列以利用直接序列扩频技术具有的优势。例如，2.4GHz物理层使用多级正交信号来发送4bit的符号，能同时支持高数据率（能够快速进入待机模式）和相对较低的数据率（最小化活跃状态时的能耗）传输。868/915MHz频段的物理层中，码片调制机制为升序余弦波二进制相移键控（Binary Phase Shift－Keying，BPSK）、半正弦波偏移四相移相键控（Offset Quadrature Phase Shift－Keying，O－QPSK），或者是根升序余弦波并行序列扩频（Parallel Sequence Spread Spectrum，PSSS）。2.4GHz频段物理层采用半正弦波偏移四相移相键控（O－QPSK）码片调制机制。此外，半正弦O－QPSK维持一个比例为1的峰值平均功率比，能够尽可能降低系统的功耗和实现的复杂度。

3.1.3 使用直接序列扩频

直接序列扩频（DSSS）是一种增加发送信号带宽的技术。扩频技术能够改善通信质量，但要以牺牲频谱利用率为代价。例如，传统广播FM使用了一种扩频技术（宽带FM），虽然使用的不是DSSS技术，但是其得以改善的信噪比和通信质量就是扩频技术优势的一个典范。

DSSS的调制方式如下：以超过数据传输速率的速率，用预先设置好的伪随机

数字序列直接对已有的数据调制载波进行相位调制。即使频谱功率密度较低，由此产生的 DSSS 信号也将占据很宽的带宽。接收到的信号被通过复制的伪随机数字序列解调成原信号。接收器中伪随机数字序列的产生采用了一种复制技术，从而能保证自己产生的序列与发射信号中的调制紧密相关。理想状况下，复制序列能将接收到的 DSSS 信号转换成发射器中的原始数据调制载波。DSSS 将原始信号扩展成带宽更宽的信号，该信号在信道上传输后在接收端被解扩，最后恢复出原始信号和信息。

DSSS 扩频技术利用伪随机数字序列的相关特性，这样伪随机数字序列就可被用于相位调制和恢复出原始数据调制载波信号。只有使用相关的伪随机数字序列进行调制后的信号，才能够被还原成原始的数据调制载波。否则，其他调制后的信号，经过接收器中解扩频相位调制的作用，反而会被进一步扩频。

由于扩频会降低非相关调制信号的频谱功率密度，所以在接收设备附近的干扰信号、相邻信道信号以及同一信道上其他非相关扩频设备发出的信号，在其原始数据调制载波所在的窄频段上都具有较低的频谱密度。其他所有信号经过原始数据调制载波带宽过滤时，信号带宽变大、频谱密度降低、能量输出也将减少。该处理增益可用于减少对信道滤波器的要求，从而也将减少系统的实现成本。

DSSS 的成本优势源于相关信号的信噪比相对于不相关信号而言更好，但是还有其他因素同样影响着 DSSS 的成本。

相对于未扩频的数据调制载波，发射器射出的频谱扩展了的信号，其功率谱密度已被削弱，因此也就不太可能与同频段上的窄带宽服务相互干扰。正是由于该共存效应的存在，同一频段上可以实现多种不同的服务。DSSS 服务可以应用在现有频段上而不会影响现有服务，同时也不会被现有服务所影响。DSSS 技术是一种共享频段的理想技术手段。

DSSS 技术的另一个微妙优势是，其实现电路通常为大型数字电路，很少有模拟电路。而数字电路的发展遵循摩尔定律，随着集成电路光刻技术的发展，电路规模将不断缩小，这样随着时间的推移，数字电路以及无线发射器的制造成本将逐渐降低。

最后，由于 DSSS 在扩频操作上的上述有利特性，在世界范围内，众多管理部门授权在免执照的频段上使用 DSSS 技术（或者其他形式的扩频和跳频技术），当然应用要在这些管理部门的监管之下。在划分出的频段上，IEEE 802.15.4 标准利用这些分配的频段，定义了一种实用的、低功耗、低成本且免牌照的服务。

摩尔定律认为，集成电路上晶体管的数目每两年翻一番。

3.1.4 发射功率

另外，IEEE 802.15.4 标准支持任何一种被允许的输出功率。对于符合标准的设备，当廉价电池有能力为设备提供瞬时功率、设备使用高集成度低成本的片上系统（SoC）时，IEEE 802.15.4 标准要求这些设备的发射功率能够达到 -3dBm。

符合 IEEE 802.15.4 标准的典型射频芯片，可以提供的输出功率范围为 0 ~ 4dBm。要想得到更大的功率输出，需要使用一个外部功率放大电路，而这将会对整个系统的成本和功耗造成影响。

许多 IEEE 802.15.4 半导体芯片制造商设计的产品，可以提供的功率输出范围为 -10 ~ 10dBm。

3.1.5 接收灵敏度

按照规定，868/915MHz 频段物理层的射频接收灵敏度下限为 -92dBm，而 2.4GHz 频段物理层的射频接收灵敏度下限值为 -85dBm。因此，使用一个简单的接收器即可达到上述要求。简单、成本低廉的接收器，带上一个小功率的射频放大电路（功耗相对会比较大），即能满足 IEEE 802.15.4 标准的要求。

3.1.6 服务质量

为降低 IEEE 802.15.4 标准的实现复杂度，IEEE 802.15.4 标准不支持同步通信，也不支持单个 PAN 中多种不同类型的服务。然而，IEEE 802.15.4 标准支持在非竞争周期（CFP）使用可选的保证时隙（GTS），以预留网络时间来支持同步通信（避免潜在的信道访问延时）。该措施拓宽了 IEEE 802.15.4 标准的应用范围，使其可以被用到一些低通信延迟的应用中（如无线操纵杆、鼠标），以及要求更为苛刻的应用中（如工业过程控制等）。

IEEE 802.15.4 标准复杂度极低，但是其物理层支持 20kbit/s、40kbit/s、100kbit/s 和 250kbit/s 的瞬时数据传输速率。瞬时数据传输速率与数据吞吐量的高比值可以最小化设备的占空比。

总之，IEEE 802.15.4 标准被制定成实现数据交换吞吐量低、报文传输延时较长、系统实现成本低、功耗小，能够为多种应用服务提供有用的数据通信服务。

3.2 IEEE 802.15.4 标准其他显著特性

3.2.1 网络组成

基于 IEEE 802.15.4 标准的网络，由一系列符合标准的无线设备组成。每个网络包含一个专用中央网络协调器，称为 PAN 协调器。只有 PAN 协调器可以建立新网络，并且定义网络的结构和运行模式。其他设备通过向 PAN 协调器申请，加入到网络中。除 PAN 协调器外，IEEE 802.15.4 标准定义了两种额外的逻辑设备，即协调器与网络设备。协调器为网络中其他设备提供协调服务，例如为不在 PAN 协调器覆盖范围内的网络设备提供代理服务。IEEE 802.15.4 网络由一个 PAN 协调器和至少一个网络设备组成。

IEEE 802.15.4标准定义了两种类型的设备：全功能设备（FFD）和精简功能设备（RFD）。FFD包含全部MAC服务，可以实现全部三种功能：PAN协调器、协调器或者网络设备。RFD包含精简的MAC服务，只能用作网络设备。

RFD通常采用最为简单的电路来实现，消耗最少的处理能力和内存资源。这些特性对低成本设备有着直接的影响，使其能应用到诸如照明开关、附着的传感器以及其他的应用。

3.2.2　多种网络拓扑结构

IEEE 802.15.4网络有两种基本的拓扑结构。第一种拓扑结构为星形拓扑，即网络围绕某个作为PAN协调器的全功能设备，该PAN协调器扮演着网络集线器的角色，其他全功能或精简功能设备作为网络的数据终端。此时，PAN协调器在网络中拥有一个特殊的功能，即它是网络中唯一一个能与其他多个设备有直接通信的设备。

另一种拓扑结构支持对等通信，不需要某个特定的协调器来直接干预网络连接（网络某处也会用到PAN协调器），每个设备都可以独立地建立起与其他多个设备的连接。设备可以与其他多个设备间建立直接连接，这样网络中能形成冗余路径，但系统的复杂度也随之增加。第二种拓扑结构也可以支持多种对等网络拓扑结构。

IEEE 802.15.4标准也可以支持更为复杂的簇树形网络结构，但是该种网络结构并没有被包括在IEEE 802.15.4标准之中。簇树形网络结构如图3-1所示，可以看作是网络设备簇的分层次树。簇树形网络支持更为复杂的网络连接，一定程度上简化了路由，与完全对等的互联网络相比，设备间的直接连接更少，但是这种结构会增加数据传输的时延。

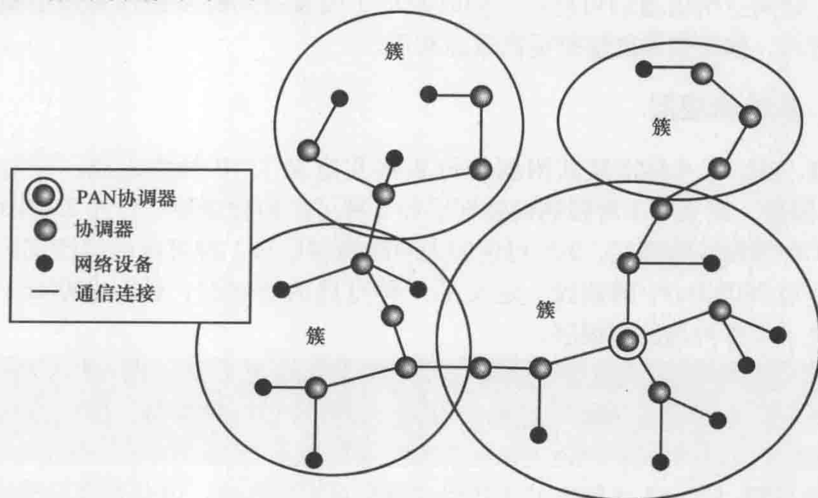


图3-1　簇树形网络结构

簇树中的叶子，即位于各层边缘的设备节点，可以是 FFD，也可以是 RFD，因为这些设备节点不需要为其他设备转发数据信息。然而，网络中其他设备节点必须是 FFD。网络中有且只有一个设备担当 PAN 协调器，在层次树中担任根节点设备的作用。PAN 协调器的选取可能是由于某个设备具有特殊的计算能力，或有与其他协议网络的桥接能力，或者简单地选取网络形成过程中第一个加入到网络中的设备。其他设备作为独立簇的根节点，称为簇头或是协调器。这些簇形成一个层次化的树，设备之间具有典型的父子节点关系。在该簇树形网络结构实例中，所有叶子节点（即位于树枝末端的设备节点）被认为是网络设备，其他位置上的设备为协调器。

基于 IEEE 802.15.4 标准对等通信建立的网络拓扑，由协议栈中的 IEEE 802.15.4 标准之外的高层来实现。本章介绍这种网络拓扑是为了显示 IEEE 802.15.4 标准的灵活性。该方面更多信息请参考本书的第 6 章。

3.2.3　信道访问

不论网络为何种类型，网络中每个设备都使用带碰撞避免的载波侦听多址访问（CSMA－CA）机制，以避免多个设备同时发送数据时的冲突。然而，信标帧的传输、保证时隙（GTS）中的传输，确认帧传输不需要使用 CSMA－CA 机制。

CSMA－CA 协议是基于射频信道可共享的自然属性。当同一信道中有两个或更多发射器同时要发送数据时，由于数据间的碰撞及相互干扰，每个发射器发送数据的成功率将减小。在射频环境中，实际干扰取决于竞争发射器的位置以及发射机各自对应的接收机。但是，对发射机而言，其竞争对手的位置信息是不可知的。为避免数据碰撞，发射机首先监听信道，待信道空闲后再发送数据。载波侦听增加了访问空闲信道的可能性，同时减小了因数据同时发送而碰撞的概率。按照这种方式，信道资源能够被更高效地利用。

3.2.4　多种物理层

IEEE 802.15.4 标准及其附属修订版本共定义了 10 种物理层：针对 868 和 915MHz 频段，定义了 1 种强制的物理层和 2 种可选的物理层；针对 2.4GHz 频段，定义了 1 种强制性物理层，3 种可选的大频段物理层和 1 种可选的线性调频扩频物理层；针对 780MHz 中国频段，定义了 1 种可选的物理层；针对 950MHz 日本频段，定义了 2 种可选的物理层。

868/915MHz 频段物理层要求符合标准的设备能够在 868MHz 和 915MHz 频段运行。该规定期望最小化市场上潜在不符合标准的设备的数量，同时也认识到了由于两频段之间的频差较小该要求需承担的成风也较低。

制定 IEEE 802.15.4 标准的工作组成员来自世界各地，因此符合标准的设备的研发和使用也是世界范围内的。为降低管理成本，IEEE 802.15.4 标准假定其设备

运行在免牌照频段上，服务受相关管理部门监管。不幸的是，世界范围内各个管理部门之间对频段的划分各不相同。有3种频段可支持此类服务，一种是世界范围内的，其他两种是地方区域性的。

对于开发者而言，频段的选择依赖于多种技术方面的考虑。虽然868MHz和915MHz频段可能比较不拥挤，也可能提供更好的服务质量，但不是世界范围内都通用的频段。针对有限市场的产品设计者，在决策时要考虑的更多的是市场和商业因素，而不是单纯的技术因素，尽管采用某种技术可能会提供更好的服务。仅选用频段不同的产品，其配送和市场成本也各不相同。同频信号干扰将引起一个问题：如何防止产品从一个管理区域移动到其他管理区域。虽然某些其他的应用（例如无线行李标签）不需要考虑区域市场策略，但是某些产品可能会需要考虑区域市场策略。

2.4GHz频段的部分波段在世界范围内是通用的，868MHz频段可在欧洲范围内通用，915MHz频段的部分波段在北美、澳大利亚、新西兰以及南美某些地区通用。在868MHz频段，IEEE 802.15.4标准定义了一个数据传输速率为20kbit/s的信道，以及两个数据传输速率分别为100kbit/s和250kbit/s的可选信道。在902～928MHz频段，IEEE 802.15.4标准定义了10个数据传输速率为40kbit/s的信道（其速率相对于868MHz频段增加了一倍），另外定义了一个数据传输速率为250kbit/s的可选信道。在2.4GHz频段，IEEE 802.15.4标准定义了16个数据传输速率为250kbit/s的信道。

修订版IEEE 802.15.4a标准定义了3个超宽带频段，频率范围分别为3～5GHz、6～10GHz和低于1GHz，提供了一种强制性的数据传输速率（851kbit/s）和三种可选的数据传输速率（110kbit/s、6.81Mbit/s和27.24Mbit/s）。此外，该修订版还定义了运行于2.4GHz频段的线性调频扩频（Chirp Spread Spectrum，CSS）物理层，其数据传输速率为1000kbit/s和可选的250kbit/s。

修订版IEEE 802.15.4c标准针对我国779～787MHz频段市场定义了全新的物理层。我国政府指定该频段用于无线传感器网络的应用，可提供250kbit/s的数据传输速率。类似的，修订版IEEE 802.15.4d针对日本市场在950～956MHz频段定义了专用物理层，可以提供100kbit/s的数据传输速率和可选的20kbit/s数据传输速率。

3.2.5 差错控制

IEEE 802.15.4标准采用简单全握手协议，以保证数据传输的可靠性和良好的通信服务质量。除了广播帧（例如信标帧）和确认帧，接收方需要对每个接收到的数据帧进行确认，从而告知发送方其发送来的报文已被接收。发送方如果没有接收到确认帧，则会重发整个数据帧。

循环冗余校验（CRC）技术被用于检测接收到的报文是否存在差错。报文的

比特位被看作一个长的二进制数，被一个相对大的素数相除。该除法的商被舍弃，该除法的余数与被除数被一起传送。接收方使用相同的大素数做相同的除法，如果算出的余数与报文中的余数相匹配，则表示报文在传输过程中未出现差错。

3.3 四种帧类型

IEEE 802.15.4 标准为数据传输定义了四种帧结构：信标帧、数据帧、确认帧和 MAC 层命令帧。每种帧结构都是一种物理层服务数据单元（PHY Service Data Unit，PSDU）。如图 3-2 所示，所有帧的结构类似，主要区别在于其用途或载荷。每个物理层协议数据单元（PPDU），由同步帧头（SHR）、物理层帧头（PHR）和物理层服务数据单元（PSDU）组成。PSDU 也即是 MAC 层协议数据单元（MPDU），作为基本的数据结构为 MAC 协议层提供服务。MAC 层协议数据单元（MPDU）包含 MAC 层帧头（MHR）、MAC 层帧尾（MFR）和 MAC 层服务数据单元（MSDU）。确认帧的 MPDU 结构例外，它不包含 MSDU。

MSDU 是帧的数据区域（如载荷），包含了该帧支持的 MAC 服务相关的数据信息，包括超帧类型、序列号、寻址信息及其他信息。

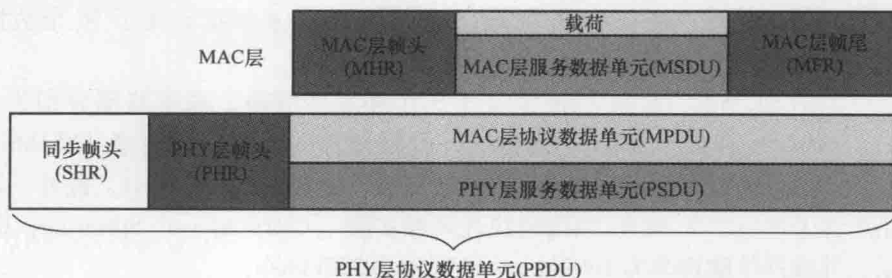


图 3-2　帧结构图

3.3.1 信标帧

不管网络采用星形拓扑、簇树形拓扑或是其他何种类型的拓扑结构，在网络中，只有全功能设备（FFD）能够发送信标帧。信标帧是 MAC 协议层服务的发起者，并且作为物理层协议的接口。信标帧有一系列用途，包括超帧边界标定、帧同步信号、联合监管等，所有这些功能都为更高层协议提供服务。

作为超帧的边界标定，信标帧提供了一个时间基准以标识超帧的边界和结构。在更高层协议中，超帧允许在信标帧之间拥有一定数量的帧。

作为帧同步信号，信标帧可以将超帧同步到某个已知的起始时间，以避免数

据发送冲突、允许接收器在没有数据发送时进入休眠、通过将一个链路中的典型传输延迟限制在一个超帧长度范围内从而达到低传输延迟的要求。此外，同步允许发送信标帧的网络设备成为链路通信的时间基准，并允许放宽个别网络设备的时间要求。

每个网络设备的时间基准可能不够精确，所以需要周期性地与发送信标帧的设备进行时间同步。

3.3.2 数据帧

不管网络采用星形拓扑、簇树形拓扑或是其他何种类型的拓扑结构，任何网络中的任何设备都可以使用数据帧。与信标帧类似，数据帧作为 MAC 协议层的服务，能够响应更高层的请求，并且作为物理层的接口。它主要将数据载荷作为一种服务提供给更高的协议层。

3.3.3 确认帧

不管网络采用星形拓扑、簇树形拓扑或是其他何种类型的拓扑结构，任何网络中的任何设备都可以使用确认帧。确认帧作为一种服务，也是 MAC 层协议服务的发起者，并且作为物理层协议的接口。它仅将对接收到的报文进行确认，为更高的协议层提供服务以实现端到端的报文控制。确认帧不包含 MAC 层载荷。

3.3.4 MAC 层命令帧

不管网络采用星形拓扑、簇树形拓扑或是其他何种类型的拓扑结构，任何网络中的任何设备都可以使用 MAC 层命令帧。与其他帧类似，MAC 层命令帧也是 MAC 协议层服务的发起者，并且作为物理层协议的接口。它将主要的监管载荷作为一种服务提供给 MAC 层协议。

针对上述四种类型帧，MPDU 被进一步封装有前导码和物理层头部，从而形成 PPDU。这种完整的数据结构允许接收方可实现帧同步并获得帧长度信息。

第4章　物理层——从字节到瓦特

物理层提供发生实际通信的物理介质接口。物理层是ISO/OSI（七层）模型的最底层，它负责提供无线电收发机控制（激活和关闭）、能量检测、链路质量、空闲信道评估、信道频率选择，以及通过物理层介质发送与接收报文[29]。

世界各国的政府都对无线电频谱进行了调控和管理。无线电频谱根据多个服务和应用来划分频段，这些服务和应用覆盖了电话、网络、军事通信、电视、电台等。在大多数情况下，每个频段的使用都需要这个频段上的特别使用许可。此外，特殊类型的频段被保留下来允许无须授权的使用，只要使用时遵从当局的规定，如输出功率限制、占空比、调制方式和其他一些参数满足约束，这些频段不需要任何特殊的许可就能使用。

世界各国的无须授权服务有所不同，但在一般情况下，设备必须符合针对每个应用的一套监管限制。发射机的每个操作都必须通过一个测试协议，以确保它们满足特定的要求。当某个特定的设计方案通过测试后，它可以得到该产品或服务的证书或型号核准。IEEE 802.15.4标准的设备就是面向型号核准的。

IEEE 802.15.4标准的实现必须符合当地国家的法律法规。例如在欧洲、日本、加拿大和美国，这些法规包括允许无须授权使用但要得到DSSS服务的型号认可。对无须授权但是要获得型号核准的限制，主要意味着遵守该频段的操作以及一些其他的特征。

IEEE 802.15.4标准被制定成使符合标准的设备能在任何三个特定的频段工作。其中两个频段被限制使用在某些特定的地理区域，而剩下的一个频段几乎是全世界通用的。这些频段的详细介绍如下：

在欧洲，欧洲电信标准组织（ETSI）发布的建议受到所有欧洲监管机构的认可，但每个服务区属于各个国家类型认可机构。在欧洲的服务区中，868.0～868.6MHz之间的频段是共有频段，它支持发送占空比小于1%的单信道低速率服务[5,6]。

在我国，我国政府最近发布了一些法规，允许在779～787MHz频段建立无须授权的无线传感器网络。同样，日本政府也批准了一个无须授权的无线传感器网络频段，但是其工作频段为850～856MHz。

在美国，对应的国家监管机构是美国联邦通信委员会（FCC）。虽然FCC只在美国有特定权限，但是FCC的规定同样被美洲和环太平洋地区的许多国家采用。与欧洲一样，有一个独立的频段——915MHz频段，覆盖在902～928MHz之间。此频段提供了几个IEEE 802.15.4信道以提供低速率服务。该频段的无须授权使用在

北美是独有的，其他地方规定此频段的使用需要授权。

为了在产品设计、市场推广和销售上获得规模经济效益，以及为了能使应用程序在不同的监管区域之间漫游，标准期望使用一个几乎在全世界通用的频段。该理想频段是无须授权的，拥有足够的带宽能提供多条信道。同时，该频段的频率足够高，这样才能设计出效率相对高的天线，否则就不能使用低成本的、高集成度的单芯片。

能满足上述要求的最好的频段是 2.4GHz 的工业、科学和医疗（ISM）频段，这个频段从 2400MHz 一直延伸到 2483.5MHz。这一频段，除极个别例外，在全球都是无须许可的。频段上的电磁波长为 12.25cm，能合理有效地使用小型天线。另外，这一频段也兼容现代硅集成电路工艺。频段的带宽也能同时提供多个相对高速率的无线电信道，使得由类似设备组成的多个独立网络能不相互干扰的共存。

IEEE 802.15.4 标准中前面所提到的各个频段都被设计成满足规章制度的规定。比如，在 868MHz 频段，产品的占空比是有限制的。为了满足这一要求，IEEE 802.15.4 标准采用非信标模式来最小化这个频段上设备的占空比。在许多情况下，一些扩频技术被要求用于无须授权的频段。IEEE 802.15.4 使用 DSSS 服务来满足这个监管的要求，同时也使低功耗产品能实现良好的传输距离。

4.1 频段和数据传输速率

作为对区域性或全球性无须授权使用频段监管情况的反映，IEEE 802.15.4—2006 标准针对以下频段规定了几种技术：

1）868 ~ 868.6MHz 频段：该频段在大多数欧洲国家无须授权即可使用，可以提供 20kbit/s 的 BPSK 服务、100kbit/s 的 O - QPSK 服务以及 250kbit/s 的并行序列扩频（Parallel Sequence Spread Spectrum，PSSS）服务。IEEE 802.15.4 标准也称这个频段为 868MHz 频段。

2）902 ~ 928MHz 频段：该频段的某些部分在北美、澳大利亚、新西兰以及南美的一些国家无须授权即可使用，它可以提供 40kbit/s 的 BPSK、可选的 250kbit/s 的 O - QPSK 服务，以及可选的 250kbit/s 的 PSSS 服务。IEEE 802.15.4 标准也称这个频段为 915MHz 频段（用该频段的中间频率来代表）。

IEEE 802.15.4 标准 868/915MHz 频段的物理层需要设备都能兼容地工作在 868MHz 频段和 915MHz 频段。对于该标准的目的而言，868/915MHz 频段可以被认为是单一的连续的频段。

3）2.4000 ~ 2.4835GHz 频段：该免授权频段可以为世界大多国家提供 250kbit/s 的 O - QPSK 服务。该频段被称为 2.4GHz 频段。

IEEE 802.15.4—2006 标准的修订版增加了一些其他频段的新物理层，主要关注新的应用领域（位置感知）或专门面向某些特定的市场区域（中国和日本）。这

些新物理层如下：

IEEE 802.15.4—2006 是原始标准 IEEE 802.15.4—2003 的修订版，其在较低频段中添加了两种额外的调制方式选项：O-QPSK 和 PSSS。这种新的物理层选项相比以前提供了较高的数据速率。

1）修订版 A：三个设计成支持多操作区域的位置感知应用的超宽带频段：250~750MHz，3.1~4.8GHz，6.0~10.6GHz；一个 2.4GHz 频段的线性调频扩频（CSS）物理层。

2）修订版 C：779~787MHz：此频段在我国是免授权的，能提供 250kbit/s 的 O-QPSK 服务和 250kbit/s 的 MPSK 服务。

3）修订版 D：950~956MHz：此免授权频段是针对日本市场的，能提供 100kbit/s 的 GFSK 服务和 20kbit/s 的 BPSK 服务。

由于 2.4GHz 频段几乎在全球都可免费使用，因此 2.4GHz 的物理层成为 IEEE 802.15.4 应用的首选，尤其是那些需要在不同地区之间流通使用的产品。即使对于非移动应用而言，2.4GHz 频段也提供了规模、分销和营销的一些优势：一个单一的产品可以销往全球多个地方而不用考虑当地的法规限制，这能够降低生产成本，同时也省去了跟踪多种产品到多个目的地的供应链费用。

由于 IEEE 802.15.4a（修订版 A）具有略有不同的应用重点和技术的复杂性，此书没有介绍包括 CSS 在内的超宽带物理层技术。对于有兴趣的读者，修订版 A 提供了大量的介绍性内容。

然而，由于某些相同的原因，许多其他应用都使用了 2.4GHz 频段，从微波炉到无线个域网（WPAN）和无线局域网（WLAN）。由此产生的拥塞对于某些应用和市场是不能接受的。为了解决这个问题，IEEE 802.15.4 提供了其他可以被使用的频段，譬如为欧洲提供了 868/915MHz 频段，为我国提供了 780MHz 频段，或日本的 950MHz 频段。有了这个功能，系统设计工程师们可以使用这种区域性的频段，从而避免 2.4GHz 频段的拥塞。这些区域性的频段对于某些应用来说可能是一个很好的设计选择，例如，电表读数应用本质上具有地域性和有限的移动性。同样的，不同的传感器在不同的应用领域里也可以使用此项功能。

IEEE 802.15.4 被设计成在有意辐射体（如其他无线电系统）或无意辐射体（如微波炉）引起的干扰环境中，还能有效地提供高可靠性的通信，这些都将会在接下来的章节里叙述。

4.1.1　数据率

由于各频段的物理特性和当地规定的不同，IEEE 802.15.4 标准针对不同的频段规定了多种不同的数据传输速率和调制方式。每个频段对应的数据传输速率

（比特和符号）和调制参数见表 4-1。

表 4-1　IEEE 802.15.4 标准的频段和调制参数 IEEE 802.15.4—2006

频段	频率范围	比特率	符号率	DSSS 扩频参数	
				调制	码片速率
868MHz	868 ~ 868.6MHz	20kbit/s	20ksymbols/s	二进制相移键控（BPSK）	300kchip/s
		100kbit/s	25ksymbols/s	偏移四相移相键控（O-QPSK）	400kchip/s
		250kbit/s	12.5ksymbols/s	并行序列扩频（PSSS）	400kchip/s
915MHz	902 ~ 928MHz	40kbit/s	40ksymbols/s	二进制相移键控（BPSK）	600kchip/s
		250kbit/s	62.5ksymbols/s	偏移四相移相键控（O-QPSK）	1Mchip/s
		250kbit/s	50ksymbols/s	并行序列扩频（PSSS）	1.6Mchip/s
2.4GHz	2.4 ~ 2.4835GHz	250kbit/s	62.5ksymbols/s	偏移四相移相键控（O-QPSK）	2Mchip/s

修订版 A

频段	频率范围	比特率	符号率	调制
超宽带 1	250 ~ 750MHz	110kbit/s	0.12MHz	带二进制相移键控（BPSK）的脉冲位置调制（BPM）
		850kbit/s	0.98MHz	
		1700kbit/s	1.95MHz	
		6810kbit/s	7.8MHz	
		27240kbit/s	15.6/31.2MHz	
超宽带 2	3.1 ~ 4.8GHz	110kbit/s	0.12MHz	
		850kbit/s	0.98MHz	
		1700kbit/s	1.95MHz	
		6810kbit/s	7.8MHz	
		27240kbit/s	15.6/31.2MHz	
超宽带 3	6.0 ~ 10.6GHz	110kbit/s	0.12MHz	
		850kbit/s	0.98MHz	
		1700kbit/s	1.95MHz	
		6810kbit/s	7.8MHz	
		27240kbit/s	15.6/31.2MHz	
2.4GHz	2.4 ~ 2.4835GHz	250kbit/s	166.67ksymbols/s	线性调频扩频（CSS）
		1000kbit/s		

修订版 C

频段	频率范围	比特率	符号率	DSSS 扩频参数	
				调制	码片速率
780MHz	779～787MHz	250kbit/s	62.5ksymbols/s	偏移四相移相键控（O-QPSK）	1000kchip/s
				多进制移相键控（MPSK）	

修订版 D

频段	频率范围	比特率	符号率	DSSS 扩频参数	
				调制	码片速率
950MHz	950～956MHz	20kbit/s	20ksymbols/s	二进制相移键控（BPSK）	300kchip/s
		100kbit/s	100ksymbols/s	高斯频移键控（GFSK）	不适用

在 868MHz 频段，强制性的基本数据传输速率是 20kbit/s，但是开发人员可以额外选择数据传输速率为 100kbit/s 的 O-QPSK 调制技术或数据传输速率为 250kbit/s 的 PSSS 调制技术。同理，在 915MHz 频段，强制性的基本数据传输速率为 40kbit/s，开发人员也可以额外选择数据传输速率为 250kbit/s 的 O-QPSK 调制技术或 PSSS 调制技术。

任何工作在 868/915MHz 频段的设备，必须至少可以支持数据传输速率为 20kbit/s 或 40kbit/s 的指定调制技术，而支持更高的数据传输速率或调制技术是可选的。

当选择 950MHz 频段时，标准中两个指定的调制方案至少有一个需要被实现。为了确保在此频段的互操作性，最好是这两种调制方案都实现。

接下来的章节将对调制参数作更加详细的阐述。

4.2　信道分配

IEEE 802.15.4—2006 及其修订版 A、C 和 D 在 2450MHz 频段中定义了 16 个信道，在 915MHz 频段中定义了 30 个信道，在 868MHz 频段中定义了 3 个信道，在 2450MHz 频段中定义了 14 个重叠的线性调频扩展（CSS）信道，在 3 个 UWB 频段（500MHz 频段、3.1GHz 频段、10.6GHz 频段）中定义了 16 个信道，在 780MHz 频段中定义了 8 个信道，在 950MHz 频段中定义了 22 个信道。

IEEE 802.15.4 标准采用信道号和信道页的一个组合来指定某个无线电的工作频率。可能的信道页一共有 32 个，页编号为 0～31；而当前标准只定义了 7 个，其余的保留以供未来扩展。每个信道页被逻辑地划分为 27 个信道，编号为 0～26。第 0 信道页包含了 868MHz 频段内的 1 个信道，在 915MHz 频段内的 10 个信道，以及在 2.4GHz 频段内的 16 个信道。这些信道的中心频率见表 4-2。

表 4-2 IEEE 802.15.4 标准的信道分配，第 0 页

	信道	中心频率/MHz	应用范围
868MHz 频段	0	868.3	
915MHz 频段	1	906	
	2	908	
	3	910	
	4	912	
	5	914	
	6	916	
	7	918	
	8	920	
	9	922	
	10	924	
2.4GHz 频段	11	2405	
	12	2410	
	13	2415	
	14	2420	
	15	2425	
	16	2430	
	17	2435	
	18	2440	
	19	2445	
	20	2450	
	21	2455	
	22	2460	
	23	2465	
	24	2470	
	25	2475	
	26	2480	

IEEE 802.15.4—2006 标准引入了信道页的概念，以适应新的物理层选项和允许将来的扩展。IEEE 802.15.4—2003 标准规定的原有 27 个信道可通过第 0 信道页来访问，而新的调制机制使用各自的独立信道页。

信道页 1 包含了一个在 868/915MHz 频段上支持可选的 PSSS 高数据速率服务的信道，而信道页 2 指定了一个在该频段上支持可选的 O－QPSK 物理层服务的信道。见表 4-3，页 1 和页 2 都包括了 1 个在 868MHz 频段上运行的信道和 10 个在 915MHz 频段上运行的信道，以及余下 15 个预留的信道。

表 4-3　IEEE 802.15.4 标准的信道分配，第 1、2 页

	信道	中心频率/MHz	应用范围
868MHz 频段	0	868.3	
915MHz 频段	1	906	
	2	908	
	3	910	
	4	912	
	5	914	
	6	916	
	7	918	
	8	920	
	9	922	
	10	924	

信道页 3 和信道页 4 是为了支持 IEEE 802.15.4 标准的修订版 A（名为 IEEE 802.15.4a 标准）。见表 4-4，信道页 3 包含了可选的 CSS 物理层的信道分配，由 14 个信道组成。同样地，信道页 4 包含可选的超宽带物理层的信道分配，由 16 个信道组成，并可以分成 sub－GHz 频段、低频段、高频段这三个组。信道页 4 的信道分配详情见表 4-5。

表 4-4　IEEE 802.15.4a 标准的信道分配，第 3 页

	信道	中心频率/MHz
2.4GHz 频段 CSS	0	2412
	1	2417
	2	2422
	3	2427

（续）

	信道	中心频率/MHz
2.4GHz 频段 CSS	4	2432
	5	2437
	6	2442
	7	2447
	8	2452
	9	2457
	10	2462
	11	2467
	12	2472
	13	2484
	14～27	保留

表 4-5　IEEE 802.15.4a 标准的信道分配，第 4 页

	信道	中心频率/MHz	带宽/MHz
UWB 1 sub－GHz 250～750MHz	0	499.2	499.2
UWB 2 低频段 3.1～4.8GHz	1	3494.4	499.2
	2	3993.6	499.2
	3	4492.8	499.2
	4	3993.6	1331.2
UWB 3 高频段 6.0～10.6GHz	5	6489.6	499.2
	6	6988.8	499.2
	7	6489.6	1081.6
	8	7488	499.2
	9	7987.2	499.2
	10	8486.4	499.2
	11	7987.2	1331.2
	12	8985.6	499.2
	13	9484.8	499.2
	14	9984	499.2
	15	9484.8	1354.97
	16～27	未分配	N/A

信道页 5 是为了支持 IEEE 802.15.4 标准的修订版 C（或者叫 IEEE 802.15.4c

标准)。此页包含了4个O－QPSK信道，以及其他4个MPSK信道。同样，信道页6是支持IEEE标准修订版D，即IEEE 802.15.4d。此页包含的信道分配为10个BPSK信道和12个GFSK信道。信道页5和信道页6的信道分配详情分别见表4-6和表4-7。

表4-6 IEEE 802.15.4c标准的信道分配，第5页

	信道	中心频率/MHz	应用范围
780MHz 频段 O－QPSK	0	780	
	1	782	
	2	784	
	3	786	
780MHz 频段 MPSK	4	780	
	5	782	
	6	784	
	7	786	
	8～27	保留	

表4-7 IEEE 802.15.4d标准的信道分配，第6页

	信道	中心频率/MHz	应用范围
950MHz 频段 BPSK	0	951.2	
	1	951.8	
	2	952.4	
	3	953	
	4	953.6	
	5	954.2	
	6	954.8	
	7	955.4	
	8	954.4	
	9	954.6	
950MHz 频段 GFSK	10	951.1	
	11	951.5	
	12	951.9	
	13	952.3	
	14	952.7	
	15	953.1	
	16	953.5	
	17	953.9	
	18	954.3	
	19	954.7	
	20	955.1	
	21	955.5	
	22～27	保留	

4.3　新的可选物理层

虽然在 868/915MHz 频段上较低的数据速率有利于提高通信距离，但后果是数据吞吐量相对于 2.4GHz 频段而言较低。因此，在这些频段上运行大型网络十分具有挑战性。对于欧洲的 868MHz 频段来说，挑战不仅在于数据速率只有 20kbit/s（这是本身可用带宽有限的后果），还在于占空比的监管限制。在 868MHz 频段上工作的设备只允许以 1% 的占空比进行传输。为了弥补这一不足，IEEE 802.15.4—2006 标准增加了两个新的物理层，从而在低频段上提供了更高的数据传输速率。这两个可选的物理层为标准的实现者和用户提供了更多的选择，还使得原始设备制造商在选择解决方案时能根据应用程序的需要进行一定的性能折中。这两个新的可选的物理层，一个是在 868MHz 和 915MHz 频段上的数据速率分别为 100kbit/s 和 250kbit/s 的 O - QPSK 物理层，另一个是在这两个频段上的数据速率均为 250kbit/s 的 PSSS 物理层。为了向后兼容现有的设备，以及保证新设备之间的互操作，IEEE 802.15.4—2006 标准要求这两个方案的实现者也都要支持原来 IEEE 802.15.4—2003 标准中规定的 868/915MHz 的物理层。

在 868/915MHz 频段上，可选的 O - QPSK 物理层沿袭了 2.4GHz 频段使用的调制方案，使得实现者能共享现有无线设备的类似设计，并且使收发器工作在 3 个频段成为可能。可选的 PSSS 物理层在两个低频段上都提供了相同的数据速率，并且使用了更复杂的调制方案，其优点是改进了多径传输的性能。

此外，在上一节提到了，修订版 A 增加了四个超宽带物理层；修订版 C 增加了两个针对我国市场的可选的物理层；最后，修订版 D 添加了两个额外的可选物理层设计，以便应用于日本市场。

IEEE 802.15.4—2006 标准在低频段引入了两个新的物理层选项，从而使低频段上的吞吐量与 2.4GHz 频段上的吞吐量相当。

4.4　物理层比特层次的通信

IEEE 802.15.4 标准的物理层负责在两个设备之间建立 RF 链路。它也在发射机和接收机之间提供比特流的调制、解调和同步。最后，该物理层同时也负责分组级别的同步。

IEEE 802.15.4 标准规定了在不同频段上的几种数据速率。符合 IEEE 802.15.4—2006 标准中 868/915MHz 物理层的设备，必须支持使用 BPSK 调制技术的两种低传输速率（20kbit/s 和 40kbit/s）。该种设备也可能支持 100kbit/s 或 250kbit/s 的 O - QPSK 调制方式，或者支持 250kbit/s 的 PSSS 调制方式。2.4GHz 物

理层提供数据传输速率为 250kbit/s 的 O - QPSK 调制方案，O - QPSK 调制采用了 *m* 进制准正交调制技术。此外，修订版 A 定义了 2.4GHz 线性调频扩频的物理层，提供 250kbit/s 和 1000kbit/s 的数据传输速率。修订版 A 还定义了 3 个超宽带物理层，提供 110kbit/s、850kbit/s、1700kbit/s、6810kbit/s 和 27240kbit/s 的数据传输速率。

修订版 C 和 D 分别定义了两个额外的、工作在 780MHz 和 950MHz 频段上的、可选的物理层。符合 780MHz 物理层的设备可以支持数据传输速率为 250kbit/s 的 O - QPSK 或 MPSK 调制方式。同样的，符合 950MHz 物理层的设备支持数据传输速率为 20kbit/s 和 100kbit/s 的 BPSK 或 GFSK 调制方式。

4.4.1　2.4GHz 频段规范

IEEE 802.15.4 标准中 2.4GHz 频段的物理层采用了十六进制准正交调制技术。该调制技术使用特定的 32 位伪随机序列码元来表示 4 个比特的数据，并同时完成扩频调制。该数据调制通过环状旋转和/或共轭（反转码元奇数指标）来执行。该伪随机序列在不同的地方开始，取决于调制的数据。每个码元周期内发送 4 个比特。

虽然 32 位码元可以发送 5 个比特，但选择发送 4 个比特可以尽量减少 2.4GHz 物理层实现的复杂度。所发送的 32 位码元是一个伪随机序列，只允许开始于该序列的第 4 位码元。符号 0 ~ 7 表示为 4 位码元的循环移位。符号 8 ~ 15 分别使用与符号 0 ~ 7 同样的移位，但是使用的是共轭序列（例如，奇数索引码元被反转）。

IEEE 802.15.4 标准 2.4GHz 频段的物理层规定符号率为 62.5ksymbols/s。因为每个符号可表示为 4 个比特位，所以该物理层的数据速率为 250kbit/s。待发送的 32 位码元伪随机序列，被分割到 O - QPSK 调制器的正交 I 和 Q 信道上，即偶数索引码元放置在 I 信道、奇数索引码元放置在 Q 信道。二分之一码元被放置在 Q 信道上，以创建 O - QPSK 偏移量。因为 32 位码元（现在是复合在一起的）在 1 个符号时间内被发送（16μs），所以总码元速率是 2Mchip/s。然而，在 I 或 Q 信道上的码元速率为 1Mchip/s。

起初，两个不同的伪噪声序列被用于 O - QPSK 准正交调制器上的 I 和 Q 信道，但之后它们又被组合起来将位于 I 和 Q 信道上的单一的 PN 序列分割成偶数和奇数。单个 PN 序列的优点是 I 和 Q 信道能共享一个单一的相关器，从而降低了系统实现的复杂性。

物理层中比特位级的处理包括：将 4 个比特的数据转换成一个符号，然后将该符号转换成一个循环旋转的 32 位码元序列（见表 4-8），最后将 32 位码元序列调

制到 I 和 Q 信道上。该处理过程如图 4-1 所示。

表 4-8　符号到码元的映射

数据符号（十六进制）	数据符号（二进制）（b_3 b_2 b_1 b_0）	码元值（c_0 $c_1 \cdots c_{30}$ c_{31}）
0	0000	11011001110000110101001000101110
1	0001	11101101100111000011010100100010
2	0010	00101110110110011100001101010010
3	0011	00100010111011011001110000110101
4	0100	01010010001011101101100111000011
5	0101	00110101001000101110110110011100
6	0110	11000011010100100010111011011001
7	0111	10011100001101010010001011101101
8	1000	10001100100101100000011101111011
9	1001	10111000110010010110000001110111
10	1010	01111011100011001001011000000111
11	1011	01110111101110001100100101100000
12	1100	00000111011110111000110010010110
13	1101	01100000011101111011100011001001
14	1110	10010110000001110111101110001100
15	1111	11001001011000000111011110111000

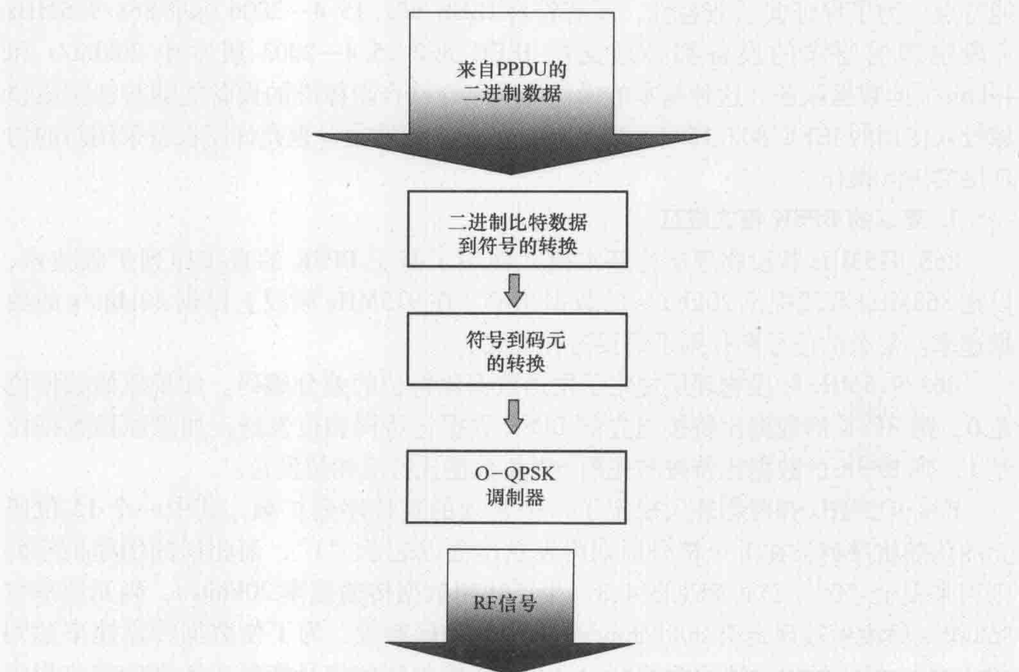


图 4-1　2.4GHz 调制和扩展

因为 32 位码元在 1 个符号时间（16μs）内被发送出去，所以总码元速率是 2Mchip/s，而每位码元的发送时间 T_c 为 0.5μs。I 和 Q 信道每隔 2 个 T_c 发送 1 位码元。

复合调制的组合包括 I 和 Q 信道之间的偏移量，如图 4-2 所示。

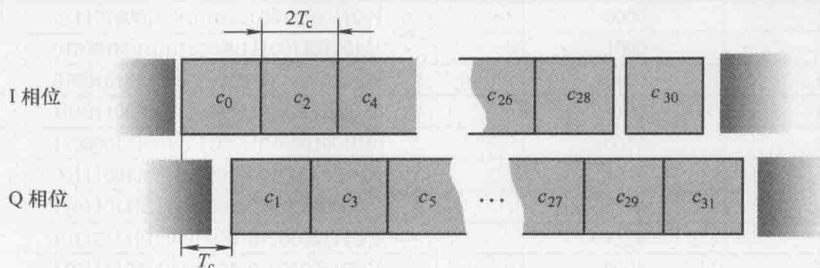


图 4-2　O－QPSK 的码元偏移量

4.4.2　868/915MHz 频段规范

IEEE 802.15.4 标准中 868/915MHz 频段物理层允许使用不同调制机制提供多种不同的数据传输速率，这样原始设备制造商可根据应用要求权衡某些功能和性能特点。为了保证向后兼容性，所有符合 IEEE 802.15.4—2006 标准 868/915MHz 频段物理层要求的设备都必须支持 IEEE 802.15.4—2003 版本中 20kbit/s 和 40kbit/s 的数据服务。这种基本的操作模式允许符合新标准的设备能够与已在该领域投入使用的 IEEE 802.15.4—2003 标准的设备相通信，也允许新设备采用新的物理层实现互操作。

1. 要求的 BPSK 模式规范

868/915MHz 频段物理层的基本模式使用了基于 BPSK 的直接序列扩频技术，以在 868MHz 频段提供 20kbit/s 的数据速率，在 915MHz 频段上提供 40kbit/s 的数据速率。复杂的信号路径则不需要这种模式。

868/915MHz 频段物理层规定了发送数据比特位的差分编码。如果原始数据位是 0，则 BPSK 的数据比特按与先前 BPSK 数据比特同相位发送；如果原始数据位是 1，则 BPSK 的数据比特按与先前 BPSK 数据比特反相位发送。

868/915MHz 频段物理层规定了一个常规的直接序列扩频，其中一个 15 位码元的伪随机序列被在 1 个符号周期内发送出去以表示“1”，而相反的伪随机序列则用来表示“0”。该过程见图 4-3。为了达到数据传输速率 20kbit/s，码元速率在 868MHz 频段中被规定为 300kchip/s；在 915MHz 频段，为了使数据传输速率达到 40kbit/s，指定的码元速率为 600kchip/s。将接收到的信号恢复成数据的接收程序如图 4-4 所示。

输入数据　数据　PN　PN码　f_x　调制

		载荷	
		868MHz	915MHz
T_b	比特周期	50μs	25μs
R_b	比特率	20kbit/s	40kbit/s
T_c	码元周期	3.33μs	1.66μs
R_c	码元率	300kbit/s	600kbit/s
N_c	每个符号的码元数	15	

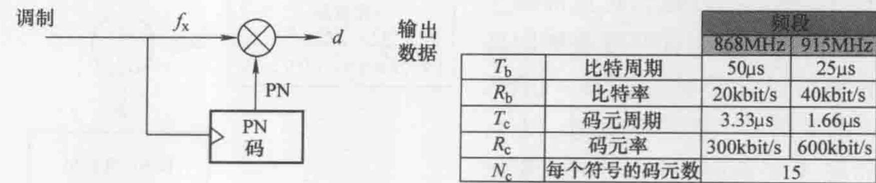
时间　频率

T_b　比特　数据　+　−　$-R_b$　R_b　f

T_c　码元　PN　$N_c T_c$　$-R_c$　R_c　f

T_c　f_x　$-R_c$　R_c　f

图 4-3　DSSS 调制



		频段	
		868MHz	915MHz
T_b	比特周期	50μs	25μs
R_b	比特率	20kbit/s	40kbit/s
T_c	码元周期	3.33μs	1.66μs
R_c	码元率	300kbit/s	600kbit/s
N_c	每个符号的码元数	15	

图 4-4　DSSS 解调

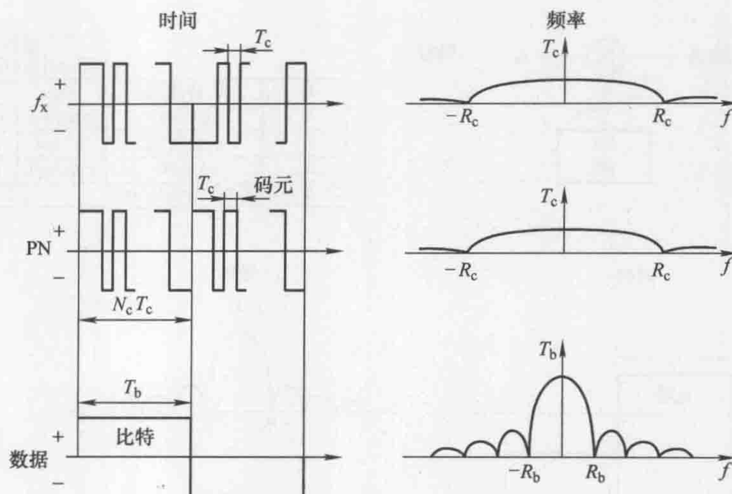


图 4-4　DSSS 解调（续）

图 4-5 描述了 868/915MHz 频段的调制和扩频过程。

BPSK 调制使用了一个不同的 PN 序列，但是在两个较低数据速率时共享一个 PN 序列。这两种数据速率的差异是由于不同的码元速率造成的，但是二者在每个数据位代表的码元数和码元模板方面是相同的。

2. 可选的 O－QPSK 模式规范

在较低频段上可选的 O－QPSK 调制机制源于 2.4GHz 物理层所使用的 O－QPSK 调制机制，它在 868MHz 频段的数据传输速率为 100kbit/s，在 915MHz 频段的数据传输速率则为 250kbit/s。它允许 868/915MHz 频段上的 BPSK 模式的数据吞吐量得到显著提高，同时还可以让开发者利用高频段的相似设计经验。该 O－QPSK 调制技术采用一个接近正交的、十六进制的准正交调制机制，即使用 16 码元的伪随机噪声序列将每 4 个比特位调制成一个符号。与 2.4GHz 频段物理层类似，码元序列的循环移位和/或共轭被用来调制数据。符号 0～7 表

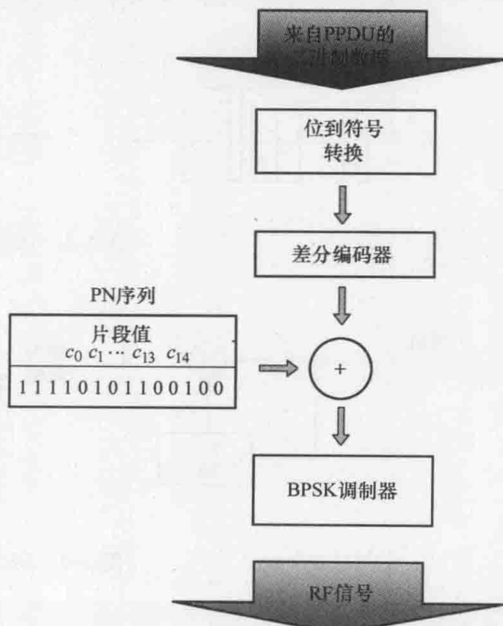


图 4-5　868/915MHz 频段的调制与扩展过程

示为 2 位码元的循环移位。符号 8 ~ 15 分别使用符号 0 ~ 7 同样的移位，但是使用的是共轭序列（例如，奇数索引码元被反转）。此调制方案中的码元序列见表 4-9。

表 4-9 可选的 O – QPSK 调制中符号到码元的映射

数据符号（十六进制）	数据符号（二进制）(b_3 b_2 b_1 b_0)	码元值 (c_0 c_1 $\cdots c_{14}$ c_{15})
0	0000	0011111000100101
1	0001	0100111110001001
2	0010	0101001111100010
3	0011	1001010011111000
4	0100	0010010100111110
5	0101	1000100101001111
6	0110	1110001001010011
7	0111	1111100010010100
8	1000	0110101101110000
9	1001	0001101011011100
10	1010	0000011010110111
11	1011	1100000110101101
12	1100	0111000001101011
13	1101	1101110000011010
14	1110	1011011100000110
15	1111	1010110111000001

这个新的可选的 O – QPSK 物理层与基本模式相比提供了更高的数据吞吐量，同时还可以让开发者共享 2.4GHz 频段的已有相似设计经验。

可选的 O – QPSK 在 878MHz 频段上的符号率为 25ksymbol/s，而码元速率则为 400kchip/s；在 915MHz 频段上的符号率为 62.5ksymbol/s，而码元速率则为 1Mchip/s；这样才能产生前文提到的 100kbit/s 和 250kbit/s 的数据服务。在传输前，符号被分割到调制器的 I 和 Q 信道上。偶数索引的码元要被放置在 I 信道中，同样，奇数索引码元要被放置在 Q 信道中。I 和 Q 信道的传送需要半位码元周期偏移，即偶数索引码元放置在 I 信道、奇数索引码元放置在 Q 信道。I 和 Q 信道的传输存在半位码元周期的偏移。

此调制过程与图 4-1 所示的某个 2.4GHz 频段物理层相同。复杂的调制机制及其偏移量如图 4-6 所示。

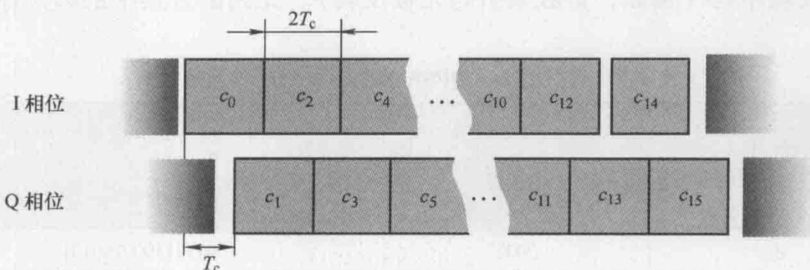


图 4-6 针对 868/915MHz 频段物理层 O－QPSK 的码元偏移量

3. 可选的 PSSS 模式规范

可选的并行序列扩频（PSSS）物理层，基于幅移键控（ASK）采用了多码调制方案[22]。PSSS 模式的优点在于：相比其他两个较低频段物理层，该模式提供了一种改良的多径性能，同时也可以在 868MHz 和 915MHz 频段达到与 2.4GHz 频段物理层相同的数据传输速率。然而，它的缺点是收发器的设计相比其他可选物理层要稍微复杂些。

该新的可选 PSSS 物理层比基本模式提供了更高的数据吞吐量，同时由于使用了先进的多码调制机制而提高了性能特性。

PSSS 模式物理层采用了 31 位码元的基础序列。为了适用于 868MHz 频段，此序列被旋转了 1.5 位码元，然后添加一位码元的循环扩展，这样就可以形成 20 个几乎正交的伪随机序列，该序列的长度为 64 个半码元长。PSSS 模式在 868MHz 频段所使用的编码表见表 4-10。对于 915MHz 频段，该序列通过 6 位码元和 1 个扩展码元来循环位移，此操作会形成 5 个长度为 32 位码元的几乎正交的伪随机序列。PSSS 在 915MHz 频段使用的代码序列见表 4-11。该调制过程包括：获取物理层的头部及其在有效载荷的二进制数据，并将其中 20 个数据位（在 868MHz 频段上）和 5 个数据位（在 915MHz 频段上）转换成符号。如果最后一个符号的长度少于要求的长度，那么“0”将被填充到最后一个符号以填满该符号。符号对应的每个比特位都被转换成双极性的信号，即位“1”变成了位“+1”，位“0”变成了位“-1”。接着执行符号到码元的转换，然后执行 ASK 调制，如图 4-7 所示。在此调制过程中，符号中第一个比特位的双极性表达式被乘以对应的 PSSS 代码表中的第一序列，符号中第一个比特位的双极性表达式被乘以对应的 PSSS 代码表中的第二序列，以此类推。其结果是，各自的 PSSS 代码序列取决于数据位，要么被反转或没有被反转。

表 4-10　868MHz 频段 PSSS 编码表

序列号	码元号																															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	−1	−1	−1	−1	1	−1	−1	1	−1	1	1	−1	−1	1	1	1	1	1	−1	−1	−1	1	1	−1	1	1	1	−1	1	−1	1	−1
1	1	1	−1	1	−1	1	−1	−1	−1	−1	1	−1	−1	1	−1	1	1	−1	−1	1	1	1	1	1	−1	−1	−1	1	1	−1	1	1
2	−1	−1	1	1	−1	1	1	1	−1	1	−1	1	−1	−1	−1	−1	1	−1	−1	1	−1	1	1	−1	−1	1	1	1	1	1	−1	−1
3	1	1	1	1	1	−1	−1	−1	1	1	−1	1	1	1	−1	1	−1	1	−1	−1	−1	−1	1	−1	−1	1	−1	1	1	−1	−1	1
4	1	−1	1	1	−1	−1	1	1	1	1	1	−1	−1	−1	1	1	−1	1	1	1	−1	1	−1	1	−1	−1	−1	−1	1	−1	−1	1

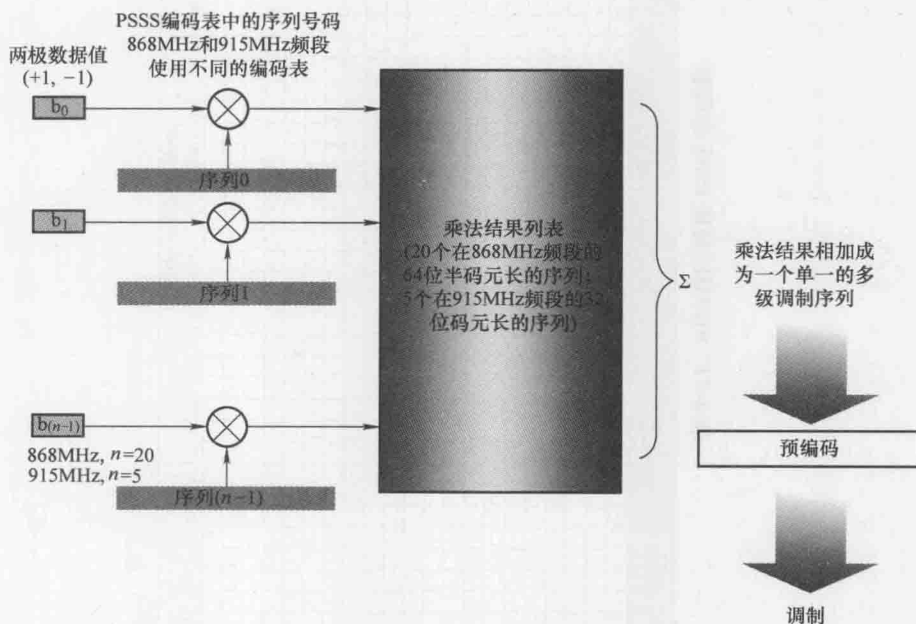


图 4-7　PSSS 模式物理层的符号到码元映射

这些乘法的结果（20 个在 868MHz 频段的相乘结果和 5 个在 915MHz 频段的相乘结果）相加成为一个单一的多级调制序列。随后是一个两步骤的预编码过程，以消除多级调制序列中的直流分量以及规范化该序列。为了在介质上传输该序列，幅移键控（ASK）被用来将该序列调制到某个载波上。

同步帧头使用 BPSK 调制，以相同的码元速率和脉冲（被用于物理层帧头和载荷）来传输。图 4-8 显示了 PSSS 模式物理层的调制和扩频功能。

表 4-11　915MHz 频段 PSSS 编码表

Sequence Number	Chip Number 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	
1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1
2	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	
3	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1
4	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	
5	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1
6	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	
7	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1
8	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	
9	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1
10	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	
11	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1
12	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	
13	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	-1	-1
14	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1	1	
15	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	-1	1
16	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1	1	
17	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	-1	-1
18	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	
19	-1	-1	1	-1	-1	1	-1	1	1	-1	-1	1	1	1	1	1	-1	-1	-1	1	1	-1	1	1	1	-1	1	-1	1	-1	-1	-1	-1

Half-chip Number: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63

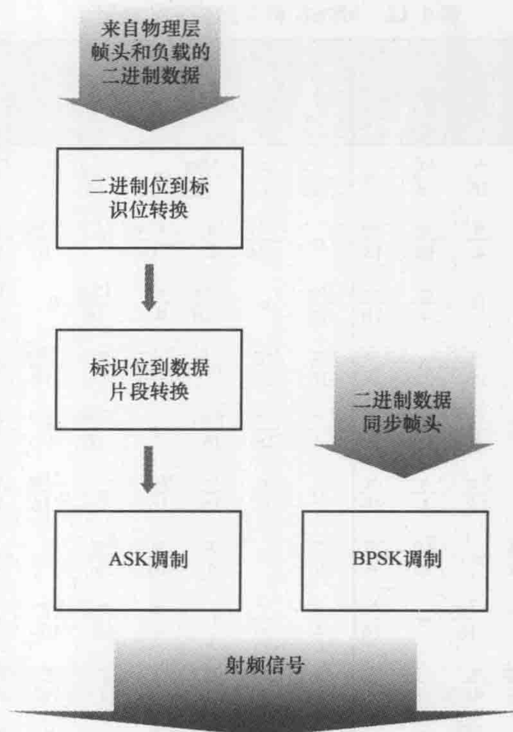


图 4-8　868/915MHz 频段的 PSSS 物理层调制与扩频

4.4.3　780MHz 频段规范

780MHz 频段的物理层规定了数据传输速率都为 250kbit/s 的两种可行的调制方案：O-QPSK 和 MPSK。

780MHz 频段的 O-QPSK 物理层采用了与 2.4GHz 频段相同的十六进制准正交调制和扩频技术，以及从符号到码元的映射和位同步。有了这个物理层，无线电码元的设计者们可以在 780MHz 频段上使用 2.4GHz 频段的已有设计。

与 O-QPSK 物理层相似，780MHz 频段的 MPSK 物理层在每个数据符号周期都采用了十六进制的正交调制技术，即 16 个正交伪随机序列中的某个序列被用来表征 4 个比特的信息数据；然后将连续的数据符号与 PN 序列相关联起来，再运用 PSK 调制将集成的码元相位调制到载波上。表 4-12 显示了 MSPK 调制中符号到码元的映射。

4.4.4　950MHz 频段规范

950MHz 频段的物理层规定了两种数据传输速率：使用 BPSK 和直接序列扩频

的 20kbit/s 以及使用 GFSK 的 100kbit/s。

表 4-12 MPSK 符号到码元的映射

数据位（十进制）	数据位（二进制）($b_3b_2b_1b_0$)	片段值 ($c_1c_2\cdots c_{30}c_{31}$)															
0	0000	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$
1	0001	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$
2	0010	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$
3	0011	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π
4	0100	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$
5	0101	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$
6	0110	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$
7	0111	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0
8	1000	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$
9	1001	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$
10	1010	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$
11	1011	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π
12	1100	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$
13	1101	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$	$\frac{\pi}{16}$
14	1110	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0	$\frac{\pi}{4}$
15	1111	$\frac{\pi}{4}$	$\frac{\pi}{16}$	$\frac{9\pi}{16}$	π	$-\frac{7\pi}{16}$	$\frac{\pi}{4}$	$-\frac{15\pi}{16}$	0	$-\frac{15\pi}{16}$	$\frac{\pi}{4}$	$-\frac{7\pi}{16}$	π	$\frac{9\pi}{16}$	$\frac{\pi}{4}$	$\frac{\pi}{16}$	0

950MHz 频段的 BPSK 物理层使用了 868MHz 频段的 BPSK 物理层，唯一的区别是定义了更严格的功率谱密度。950MHz 频段的 GFSK 物理层将比特序列调制成一个 GFSK 载波，该载波的调制量度等于 1 并在 100kbit/s 速率时使用一个 BT 值为 0.5 的高斯滤波器。

4.5 无线电特性

IEEE 802.15.4 标准中，无线电规范被设计成允许实现低成本的数字集成电路。该规范中的大多数技术相对于其他无线技术可以被认为是放宽了要求。后续的段落会叙述 IEEE 802.15.4 无线电的一些特性。

4.5.1 输出功率

IEEE 802.15.4 标准提供了一个广泛的发射机功率输出范围，符合该标准的设备必须能够发射出 -3dBm 的信号。输出功率的上限由当地的管理机构设定。例如在美国，在 2.4GHz 频段下采用 DSSS 的发射机功率可以达到 1W[25]；而在欧洲，在相同频段的最大发射功率为 100mW[7]。

4.5.2 灵敏度

对于 2.4GHz 频段的物理层、780MHz 频段可选的 O-QPSK 物理层、868/915MHz 频段的 PSSS 物理层、950MHz 频段 GFSK 物理层，IEEE 802.15.4 标准规定接收机必须能够正确解码输入功率为 -85dBm 或更低的信号。对于较低频段的 BPSK 物理层，接收机必须能够正确解码输入功率为 -92dBm 或更低的信号。IEEE 802.15.4 标准并没有限制更好的灵敏度。

一种天线有一个恒定的有效孔径，并且此类天线的增益会随着工作频率的增加而增加。抛物面天线就是这样的一个例子：当发射机和接收机在其通信线路上采用固定尺寸的抛物面天线时，用户会发现随着工作频率的增加通信范围也随之变大。而当使用偶极子天线时，情况则与此相反。

4.5.3 通信范围

在自由空间中，发射机和接收机之间的路径损耗取决于它们之间的通信距离，而与使用的频率无关。IEEE 802.15.4 标准定义的频段之间没有内在差异。然而，使用的天线类型不同，各自的路径损耗和频率也会有差异：一个固定增益的天线，诸如半波偶极子天线，有一个因工作频率增加而减小的有效孔径（区域），此偶极天线随着频率的增加而物理尺寸越小，从而导致即其有效面积减少。在较高频率下，此偶极天线因此可以截获较少的已发送的信号，从而在其终端产生较少的接收信号。当发射机和接收机在其通信线路上采用偶极子天线时，用户会发现随着工作频率的增加，通信覆盖的范围也随之变大，不过其原因更多是在于所采用的天线，而非路径上的损耗。

尽管如此，许多 IEEE 802.15.4 标准的实现期望采用固定增益（偶极子）天线。对于这些实现，Friis 模型给出了在自由空间里，接收端的天线可用功率与发

送端天线的功率的比值：

$$\frac{P_R}{P_T}=G_T G_R\left(\frac{\lambda}{4\pi d}\right)^2=G_T G_R\left(\frac{c}{4\pi f d}\right)^2 \tag{4-1}$$

式中，P_R 和 P_T 分别代表接收端天线和发送端天线的功率值，单位为 W；G_R 和 G_T 分别为接收端天线和发送端天线的增益值；λ 是信号的波长，单位为 m；f 是信号的频率，单位是 Hz；d 是接收端和发送端之间的距离，单位为 m；c 是光速，单位为 m/s。

假设使用的是恒定增益的天线，当这些常量取合适值的时候，此公式可以被表示为一个基本的发送天线端到接收天线端的损耗 L_B（dB），其以分贝（dB）的形式表达如下：

$$L_b=32.44+20\ \lg df_{MHz}+20\ \lg d_{km} \tag{4-2}$$

式中，损耗 L_b 的来源包括天线有效面积（随着频率的减小而减小）和路径损耗（它是与频率相关的常数）。这里，我们假定天线的增益是恒定的，我们将 G_R 和 G_T 归一化为 1。为了进一步简化，我们把 780MHz、868MHz、915MHz 和 950MHz 频段都近似为 1GHz 频段，把 2.4GHz 频段近似为 2GHz 频段，这样，损耗可以表示成为

$$L_{b@1GHz}=92+20\lg d_{km} \tag{4-3}$$

$$L_{b@2GHz}=98+20\lg d_{km} \tag{4-4}$$

IEEE 802.15.4 标准中，物理层规定在 1GHz 频段左右的接收灵敏度至少为 -92dBm，当发射机的发射功率为 0dBm 时，最大自由传播空间范围大约为 1km（lg1 = 0）。在相同条件下，如果物理层规定接收灵敏度至少为 -85dBm 时，对于同样功率的发射机，此时最大自由传播空间范围大约只有 450m。

对于较高的 2.4GHz 频段，接收机的灵敏度必须达到 -85dBm，当发射机的发射功率为 0dBm 时，通过类似的计算可以得出最大自由传播空间范围大约为 220m。值得再次注意的是，传播距离的差异完全取决于所用天线的种类。

这些传播距离都是在自由空间、天线完全匹配、全向增益天线、无干扰的条件下得出的，代表了理论上的最大传播距离。自由空间传输模型没有考虑一些环境参数对无线电传播的影响，这些影响包括波的反射、衍射和散射。一种在真实环境中模拟 RF 信道的传播行为的常用模型是对数正态阴影模型。图 4-9 显示了典型的室内传播效应图，以及由于遮蔽而产生的距离变化（报文的输出功率为 0dBm），该图形分别显示了在 915MHz 和 2.4GHz 频段上接收到的各向同性的功率与距离之间的关系。从这些图可以看出，距离随着频率的增加而减小，我们在分析中还是假设天线是恒定增益的。同样的，图中的变化率是一个无线信道的特性函数。在室内环境中，路径损耗系数典型值通常是 $n=2$ 或 $n=4$。另外，接收功率的室内方差一般是从 $\sigma=3$ 到 $\sigma=11$。

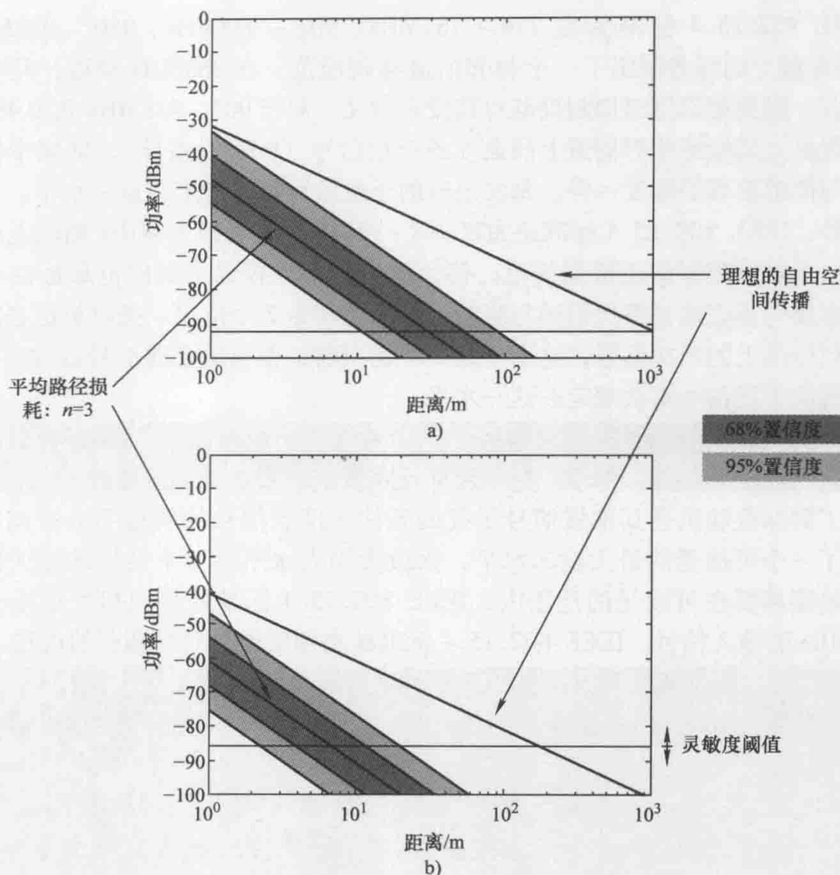


图4-9 正态分布时的典型室内传播距离（0dBm发射功率）
a）915MHz b）2.4GHz

要知道以前的结论都是使用自由空间无线传播模型推导出来的。这些计算都是理想化的；确保你已读完实际传输模型这个章节。

4.5.4 接收机的选择性

根据定义，DSSS信号是调制数据信号的一个宽带变量。我们已经讨论过DSSS扩频通信的优点，它提供了一个宽松的无线电选择性。此外，IEEE 802.15.4信道间隔（在2.4GHz频段为5MHz）相对于它们自己的带宽（3MHz；在2.4GHz频段约1.5MHz的噪声带宽）较大。随着0dB的相邻信道要求，以及更远相邻通道相对宽松的要求，开发者需要进行少量的选择以达到系统的要求。

4.5.5 信道的选择性与阻断

IEEE 802.15.4 标准为在 779 ~ 787MHz、902 ~ 928MHz、950 ~ 956MHz 和 2.4GHz 频段上的服务制定了一个相邻信道抑制规范。在 868MHz 频段，只有一个信道存在，因此相邻信道抑制规范对其没有意义。对于 902 ~ 928MHz 和 2.4GHz 频段，接收机必须拒绝相邻信道上同强度的干扰信号（0dB 的差异），即该干扰信号的强度与信道信号的强度一样。每次出现的干扰信号都被规定在这一水平。

此外，IEEE 802.15.4 标准还为在 902 ~ 928MHz 频段和 2.4GHz 频段上的服务制定了一个替代相邻信道抑制规范。替代信道是指与相邻信道离得最近的一个信道，或者换句话说就是替代信道与当前工作信道相距 2 个信道。接收机也必须能够拒绝替代信道上的干扰信号，这个干扰信号比当前工作信道上的信号强度高 30dB。每次出现的干扰信号都被规定在这一水平。

对这些干扰信号强度的规定确保了多个共处一个区域的 WPAN 在各自占用不同信道时的通信可靠性。单个干扰信号的规定反映了相对低的流量。

为了确保接收机在其他强信号干扰的条件下接收信号的质量不会变差，该规范提供了一个可接受的最大输入水平，该最大输入水平绝对不会导致过大的错误率。当错误率要在可接受的范围内，IEEE 802.15.4 标准的接收机须能承受至少为 -20dBm的输入信号。IEEE 802.15.4 标准的物理层没有对互调制的规定。

IEEE 802.15.4 标准定义了如下四种类型的服务原语：

1）请求（Request）：请求原语由呼唤层（也称作用户层）发出以请求某个服务。

2）指示（Indication）：指示原语由服务层传递给用户层，以指示一个内部事件的意义。此事件可能与某个远程服务请求逻辑上相关，或由某个服务层的内部事件引起。

3）响应（Response）：响应原语由用户层传递给服务层，以完成由之前某个指示原语引起的过程。

4）确认（Confirm）：确认原语由服务层传递给用户层，以传达一个或多个与以前服务请求相关联的结果。

4.6 物理层服务

IEEE 802.15.4 标准的物理层（PHY）通过使用两个服务，在物理无线信道和 MAC 子层之间提供了一个接口。这两个服务是 PHY 数据服务和 PHY 管理服务（被称为 PHY 层管理实体或 PLME），可分别通过物理层数据服务访问点（PHY Layer Data Service Access Point，PD - SAP）和物理层管理实体服务访问点（PHY Layer Management Entity Service Access Point，PLME - SAP）进行访问。

PHY 层具有向 MAC 子层提供服务的能力。

4.6.1　PHY 层数据服务

PHY 层数据服务为 MAC 子层提供了三种原语：PD - DATA. request、PD - DATA. confirm 和 PD - DATA. indication，如图 4-10 所示。这些 PHY 层数据服务要求一个来自对等 MAC 的响应，因此就不再需要额外的响应原语。

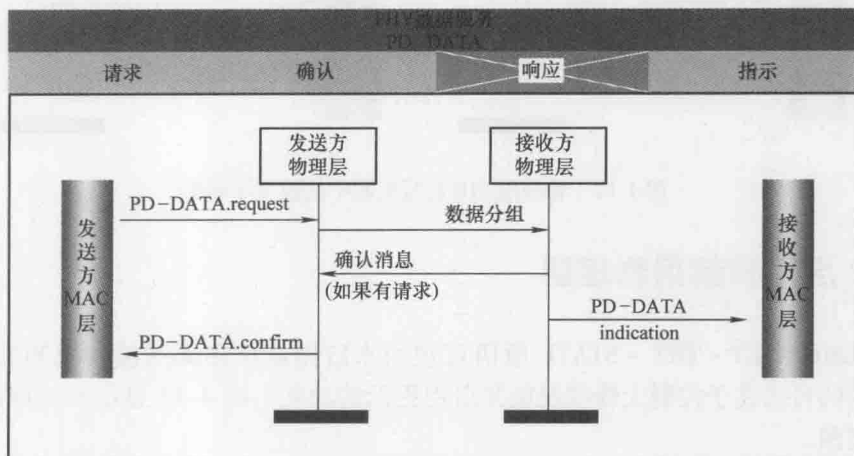


图 4-10　数据分组交换机制中的消息序列

4.6.2　PHY 层管理服务

PHY 层管理服务提供一些命令以控制通信设置和无线电控制功能。PHY 层管理实体（PLME）原语的概述见图 4-11。以下段落将会对这些原语做进一步概述。

原语	类别	描述	请求	确认	响应	指示
GET	通信设置	PHY PAN信息库管理	×	×		
SET			×	×		
SET-TRX-STATE	无线电控制	使能/关闭无线电系统	×	×		
CCA	RF能量感知	RF能量感知： 空闲信道评估 能量检测	×	×		
ED			×	×		

图 4-11　PHY 层管理服务原语

4.6.3　PHY PAN 信息库管理原语

物理层（PHY）PAN 信息库（PIB）包含了一些可配置的属性以管理物理层。PLME - GET 和 PLME - SET 原语可被用来读取或写入这些属性。

图 4-12 显示了读取或写入 PIB 属性过程的报文序列图。

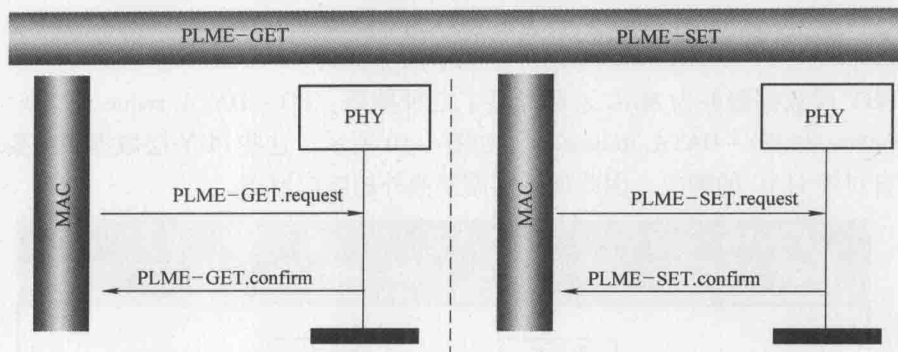


图 4-12 物理层 PIB 读写机制中的报文序列图

4.7 启用和禁用物理层

PLME-SET-TRX-STATE 原语可被用来启用或禁用无线接收机和发射机。该原语的目的在于控制无线收发机并启用更低的功耗。图 4-13 显示了该原语的报文序列图。

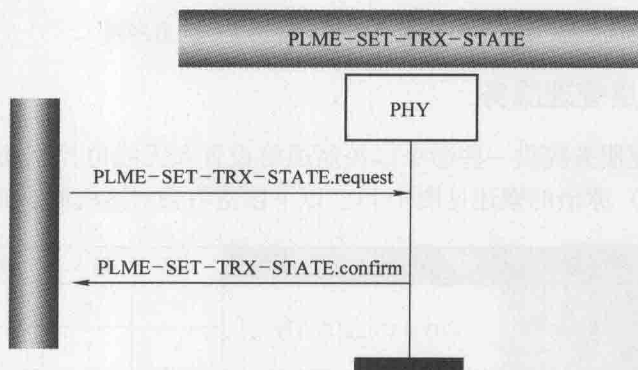


图 4-13 发送使能机制中的报文序列图

4.8 空闲信道评估

在位非信标使能网络或信标使能网络的竞争访问周期内的分组被发送之前，MAC 层指示 PHY 层在发送数据帧和 MAC 命令帧之前执行一次空闲信道评估（CCA）。

在空闲信道评估的时候，PHY 层启用接收机并执行一次 CCA 测量，然后再禁

止该接收机。当 CCA 测量完成后，PHY 层发送一个 PLME - CCA. confirm 来指示该信道是繁忙或空闲。图 4-14 显示了使用 PLME - CCA 原语的 CCA 机制，还显示了 CCA 机制的报文序列图。

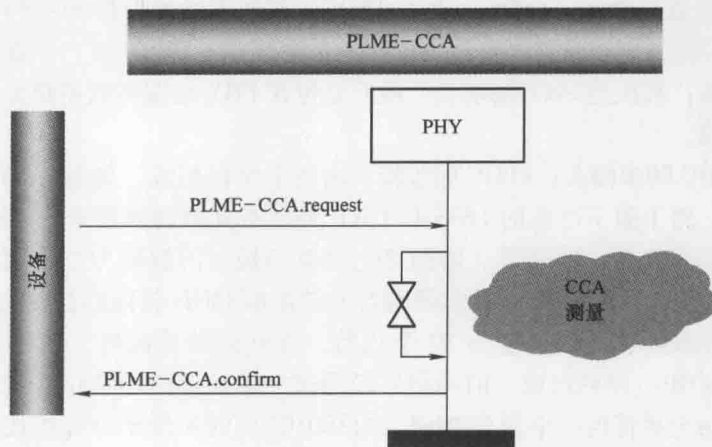


图 4-14　空闲信道评估机制中的报文序列图

4.9　能量检测

PLME - ED 原语允许一个设备在实际信道操作时执行 RF 能量检测。该能量检测与 PLME - CCA 原语中执行的测量相似，但具有更高的分辨率，它的能量取值范围为 0 ~ 255。PLME - ED 原语可以增强网络层的功能。能量检测过程的报文序列图见图 4-15。

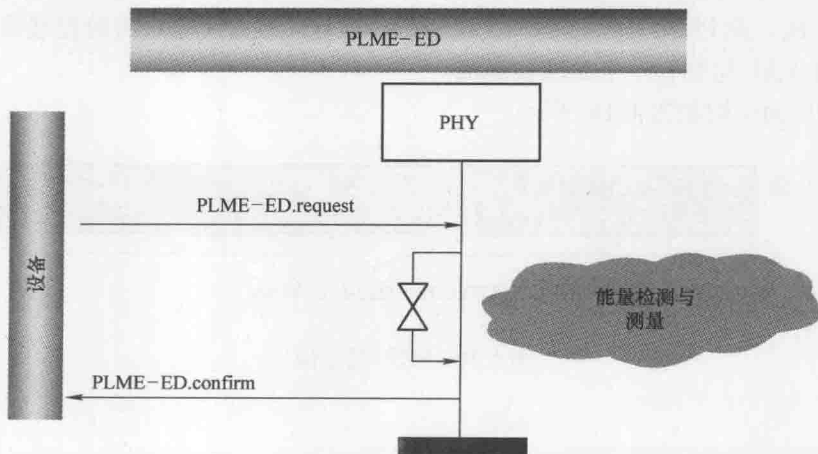


图 4-15　能量检测机制中的报文序列图

4.10 分组结构

PHY 协议数据单元（PPDU）是在 PHY 层调制无线发射器的一种分组数据结构。此 PPDU 封装所有来自于更高协议层的数据结构。PPDU 由三个部分组成：首先是同步帧头；其次是 PHY 层帧头；最后是包含 PHY 层服务数据单元的、长度可变的有效载荷。

（1）PPDU 同步帧头：PPDU 同步帧头由两个字段组成，即前导码定界符和帧起始定界符。对于除了可选的 PSSS 和 UWB 外所有其他物理层来说，前导码由 32 位组成且全部设置为二进制零（请回忆之前章节提到的解码为二进制零的码元模板）。对于可选的 PSSS 模式，其前导码当工作在 878MHz 频段时长度为 40 个比特，而工作在 915MHz 频段时长度为 30 个比特。在这两种情况时，前导码都由各自 PSSS 代码表中第一序列组成。前导码字段通过一串足够的比特位来实现码元和位同步。帧起始定界符由一个值为 0xe6（11100101）的 8 位比特流组成，并允许接收机利用该比特流定界数据报的开始。

值得注意的是，对于可选的 PSSS 模式物理层，其帧起始定界符与其他模式的物理层有所不同。PSSS 模式物理层的帧起始定界符是对应的 PSSS 代码表中第一个序列的反码。

（2）PHY 层帧头：PHY 层帧头包含一个 8 比特长的字段，该字段是最高有效位（MSB）；其余的低位字段都被用于表明帧长度信息。分组长度为 0 ~ 4 字节和 6 ~ 8字节都被保留了。长度为 5 个字节的分组是 MPDU 确认分组，长度为 9 个字节或更多的分组是 MPDU 载荷（用于 MAC 层服务）。

（3）PHY 层载荷：PHY 层载荷仅由一个被称为物理层服务数据单元（PSDU）的字段组成。此 PSDU 的长度自然是可变的，并且装载着 PPDU 的数据载荷。所有的分组在 MAC 层都有一个 MPDU 载荷。

PPDU 的结构如图 4-16 所示。

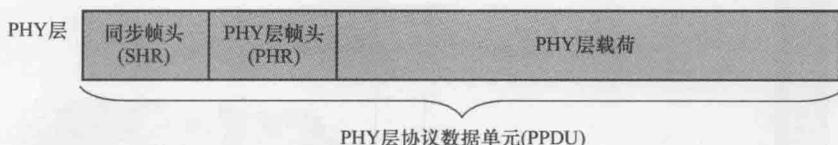


图 4-16　PPDU 的结构

第5章 媒体访问控制子层——信道接入仲裁以及更多内容

MAC子层和逻辑链路控制（LLC）子层一起，构成了ISO/OSI模型中的数据链路层（也被称为第二层）[29]。MAC层提供了对共享信道的访问控制机制，并可以提供可靠的数据传输。就无线个域网而言，对无线传输介质的优化利用是必要的，因为它们工作在有限的开放频带上，这些开放频带被包括无线局域网在内的其他几种标准或非标准的无线技术所共享。IEEE 802.15.4标准采用带碰撞避免的载波侦听多址访问（CSMA/CA）算法，该算法要求在传输之前先侦听信道以避免与其他正在进行的传输发生碰撞（一种无线通信规矩）。

IEEE 802.15.4 标准的MAC子层具有多种功能，如确认帧的产生、关联的建立与释放、安全控制、信标帧的产生以及可选的保障时隙管理（该功能可被星形网络用到）。IEEE 802.15.4标准的MAC层被设计成允许实现一个非常简单的协议栈。这有利于应用的快速发展，并对改善耗电量有直接的影响——秘诀是如此的简单。

IEEE 802标准协议集在物理层和MAC子层的规定各不相同，但在数据链路层共享一个相同的接口。这个接口是标准化的IEEE 802.2™逻辑链路控制（LLC）子层。早在无线网络标准WLAN和WPAN出台之前，标准化的LLC子层提供的这个接口就已经存在。所以，IEEE 802.15.4标准定义了业务特定会聚子层，这使得MAC层与IEEE 802.2标准之间能有适当的接口，并使得其他LLC子层的定义更适用于无线传输。IEEE 802.15.4 标准的MAC子层定义了一些通常位于LLC子层的增强功能，这样能使其适合与网络层直接连接、可以允许无线设备的简单实现。

IEEE 802.15.4 标准的MAC子层提供了对两种类型的无线网络拓扑结构的支持：星形网络拓扑和对等网络拓扑。对这些网络拓扑结构的管理是网络层的范畴，也已经超出了IEEE 802.15.4标准定义的范围。在这方面，MAC子层只执行网络层或其他更高层所要求的功能。对于应用的场景，家庭网络大多数使用星形网络拓扑，而工业和商业应用则对对等网络拓扑更感兴趣。对等网络拓扑适合构建较大的无线自组织Ad Hoc网络（主要是多跳/网状结构）。

无论网络拓扑结构如何，所有的设备都使用唯一的64位IEEE地址加入网络；这个64位的地址可以由PAN协调器分配的16位短地址代替，这样能保证它在其加入的网络里是独一无二的。本章将解释该过程的相关流程。

IEEE 802.15.4标准2006版在MAC子层上引入了一些新的改进和功能。除了

安全部分以外，所有这些新功能都是向后兼容的。IEEE 802.15.4—2006 简化和改进了安全部分，减少了安全开销。MAC 子层的其他变化包括：

1）添加了用于指示帧版本的子字段。

2）添加了一些功能以便于网络设备的同步（机制在更高层实现）。

3）让使用保障时隙成为可选的选项。

4）更新原语，从而可以使用由于新的 PHY 模式而引入的新的信道页面。

5）调度信标的开始时间，从而允许超帧的交错。

6）在信标使能网络中简化广播。

7）增加一些功能，从而减少非信标使能网络的关联时间。

通常，2006 版本中 MAC 子层的所有变化都向后兼容之前的版本。但是，也有三处变化无法向后兼容：①使用安全处理操作的 MAC 层帧；②使用信道页字段的 MAC 层帧；③MAC 层载荷大于 102 个字节的 MAC 层帧。

5.1 星形网络拓扑

在星形网络拓扑结构中，通信由一个 PAN 协调器控制。这个 PAN 协调器作为网络的主控设备，发送实现设备同步的信标帧（包括超帧控制），并且维护关联的管理。在这种拓扑结构中，网络设备只与 PAN 协调器通信，如图 5-1 所示。

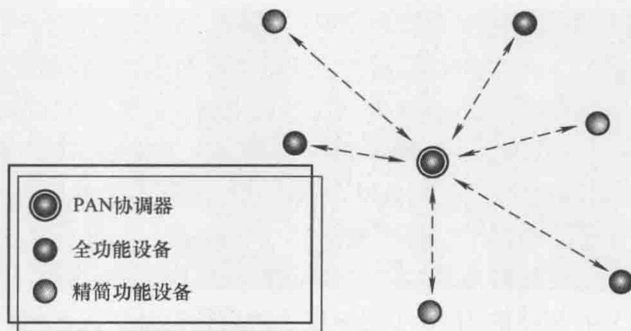


图 5-1 星形网络拓扑结构

任何全功能设备（FFD）都可以作为一个 PAN 协调器来建立自己的网络。每个星形网络的运行独立于任何相邻网络。在一个新的星形网络的形成过程中，PAN 协调器必须选择一个网络标识符（即 PAN ID），这个 PAN ID 不应被该网络周围的任何相邻网络所占用。为了实现这个目的，PAN 协调器扫描所有可用的或可选择的信道，寻找已经建立的网络，然后选择一个和它们都不同的 PAN ID。这个过程完毕后，PAN 协调器开始周期性地发送信标，允许网络设备请求加入其网络。

网络设备按照一套规定的步骤加入星形拓扑网络。首先，网络设备必须在其

通信范围内通过监听 PAN 协调器发出的信标帧来扫描可用的网络。扫描完成后，网络设备的协议栈高层向 PAN 协调器发送一个入网请求来加入一个被发现的网络。相应的，PAN 协调器决定是否允许该网络设备入网。

星形拓扑网络也支持非信标使能模式。在这种模式下，PAN 协调器发出的信标帧只有入网的功能。为了进行数据交换的网络设备同步机制是通过周期性轮询 PAN 协调器发出的数据来实现的。

5.2 对等网络拓扑

对等网络拓扑允许任何 FFD 与其射频通信范围内的其他任意 FFD 通信，并且可以通过多跳路由将报文分程传递给其射频通信范围以外的 FFD。这种拓扑结构能形成更复杂、更大的网络，包括 Ad Hoc 类型的、自组织类型的、自愈类型的结构。IEEE 802.15.4 不规定任何这些网络的细节，它只规定了 MAC 层功能以支持这些网络。

对等网络中也可以有精简功能设备（Reduced Function Device，RFD），但只能作为外围设备，因为它们不具备转发数据报的能力。因为这个原因，对等网络中必须要有足够的 FFD 来形成网络。图 5-2 显示了一个典型的对等网络。

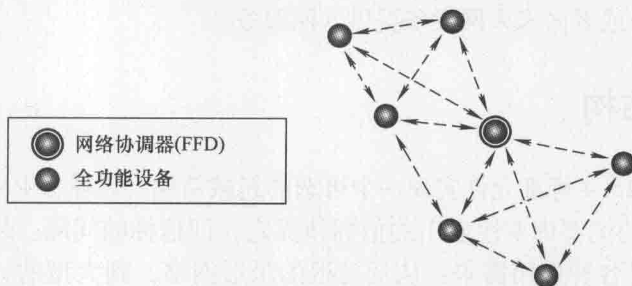


图 5-2 对等网络拓扑结构

由于需要存储更高层所需的路由表，对等通信需要额外的设备内存。

对等网络中的一个特定类型是簇树网络，其包括一些数目不定的协调器，这些协调器可以充当簇管理器，或者簇树结构的簇头，也可以充当路由器在网络中转发报文。多簇无线网络的一个主要优点是它的层次结构，该层次结构可以大大简化网络中的路由算法。图 5-3 显示了一个典型的簇树网络；该图中显示的设备包括网络设备、簇头以及管理整个网络运作的 PAN 协调器。

与星形网络的建立流程类似，任何一个 FFD 使自己成为一个 PAN 协调器，并选择一个与其附近的其他网络不同的 PAN ID ，就可以建成一个新的对等网络。在大多数情况下，对等网络是非信标使能的，但它也可以在信标使能模式下工作。

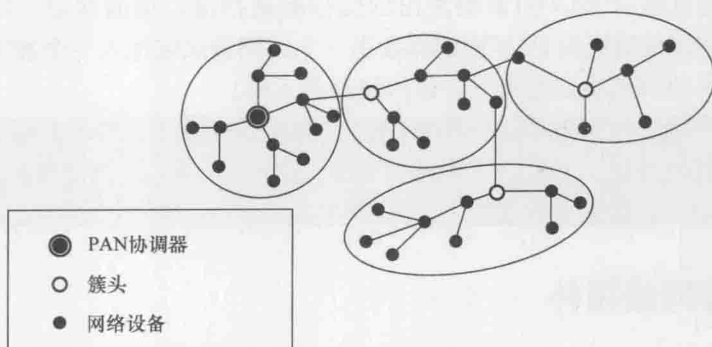


图 5-3 簇树网络拓扑结构

网络设备按照一套规定的步骤加入到对等网络：首先，具有路由功能的设备通过发现邻近 PAN 协调器或者作为 PAN 协调器代理来扫描可用的网络。IEEE 802.15.4 标准将具有路由功能的设备也认为是协调器。扫描完成后，网络设备的高层通过向 PAN 协调器或者最近的一个协调器发送入网请求来加入到一个被发现的网络。相应的，协调器决定是否允许网络设备入网。如果这个网络设备是全功能设备（FFD），它加入网络以后也可以成为一个协调器，并向其他已入网设备提供报文转发服务或者向未入网设备提供入网服务。

5.3 超帧结构

IEEE 802.15.4 标准允许实现一个可选的超帧结构。超帧由 PAN 协调器管理，其长度由 PAN 协调器周期性发出的信标帧界定，即信标帧间隔。超帧结构可被专门的配置以满足各种应用需求：从低延迟的星形网络，到大型的、长延迟的多跳网络。

每个信标帧都包含一些信息以有助于网络设备与网络的同步；这些信息包括网络标识符、信标周期、超帧结构。超帧分为 16 个连续的时隙，第一时隙起始于信标帧的开始。

需要与 PAN 协调器通信的网络设备，必须在两个连续信标帧之间内尝试完成该任务。这个时间段被称为竞争访问周期（CAP）。为了和 PAN 协调器通信，每个网络设备都需要使用基于时隙的 CSMA－CA 机制来访问信道。图 5-4 显示了一个通用的超帧结构。

一个有趣的历史注释：超帧的 16 个连续时隙最初被称为“块”。然而，该小组发现“隙”是一个更好的术语，就顺理成章地更名了。

根据要求，PAN 协调器可以将超帧中的某部分时间段专门分配给某个特定网

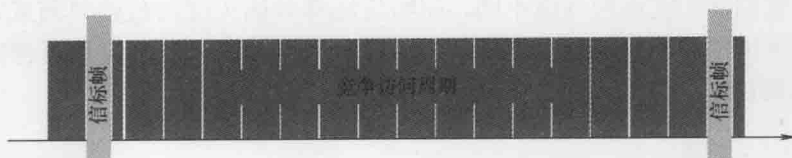


图 5-4　通用的超帧结构

络设备。这些时间段被称为保障时隙（GTS）。此功能可被用于星形网络以支持某些应用，例如某个特定带宽需求应用或较低通信延迟的应用。GTS 分组持续到超帧的结束，即下一个信标帧的开始，如图 5-5 所示。所有 GTS 构成了一个非竞争周期（CFP）。虽然 CFP 可占用超帧的大部分，IEEE 802.15.4 标准要求必须保留最少量的 CAP 部分（440 个符号），从而允许其他不使用 CFP 的设备访问通道。此规则的唯一例外是暂时减少 CAP 部分，来为了 GTS 维护而适用额外的信标长度。

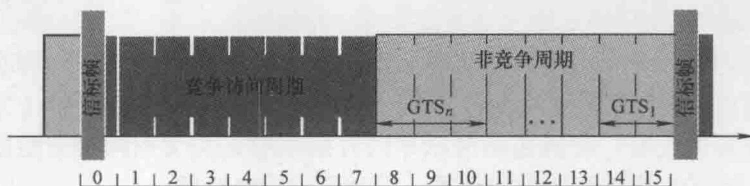


图 5-5　带 GTS 的超帧结构

每个 GTS 由整数倍个时隙组成。每个时隙长度等于两个连续信标帧之间的时间间隔的 1/16。

GTS 的分配完全由 PAN 协调器决定，但是对于要求低延迟和专用带宽的应用而言，非竞争访问是很有用的。

（1）低延迟应用：这类应用要求对有优先级的报文最小化端对端的延迟，时隙分配协议中利用优先处理和非顺序队列处理来尽量减少延迟。这样的例子包括报警条件转送或基于应用软件提供不同的服务质量（QoS）。

（2）专用带宽应用：这类应用对延时的敏感性较低，具有已知的数据流量。为每个服务分配带宽使得协议能够管理每个网络设备的队列长度。流量管理通常与 MAC 层之上的网络协议有关，但是由 IEEE 802.15.4 标准涵盖的低层必须给高层提供这个能力。

保障时隙（GTS）使更高层协议服务成为可能，但是对于那些不实现更高层次服务的网络来说，保障时隙（GTS）的使用是可选的。

对于延迟要求较为宽松的应用，超帧可以被分割成活跃和非活跃部分，而 16 个连续时隙仅占用超帧的活跃部分。超帧的非活跃部分不被用于设备之间的通信。图 5-6 显示了一种活跃和非活跃部分长度相等的情况。但是长度相等并不是必须条

件，也有它们的长度比例可能不同。超帧活跃部分的长度由超帧间隔规定，而信标帧的频率由信标帧间隔规定。例如，这样允许由电池供电的协调器构建的网络可以降低通信的占空比，同时延长协调器的电池使用寿命。

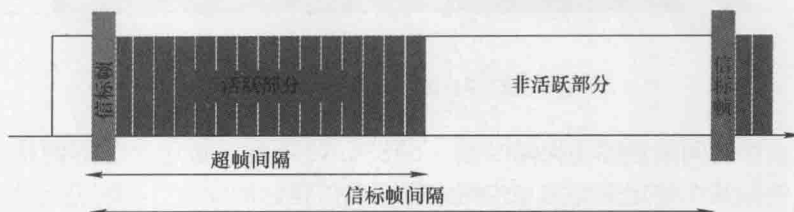


图 5-6 带活跃部分和非活跃部分的超帧结构

IEEE 802.15.4 标准 MAC 子层的一个新特点是允许一个协调器根据它从自己的协调器收到的信标帧来调度其超帧中信标帧的开始。于是，多跳网络可以使用超帧结构来让 OEM 厂商创建大型电池供电的无线网络。

该功能的另一个应用领域是针对大型信标使能的多跳网络。此功能允许多个超帧的交错或者超帧之间不会相互干扰。这种情况下，某个协调器（为其他设备提供协调服务的设备）将其超帧活跃期的开始调整到其父超帧的非活跃期。如图 5-7 所示，父节点可能是 PAN 协调器，甚至是另个协调器。

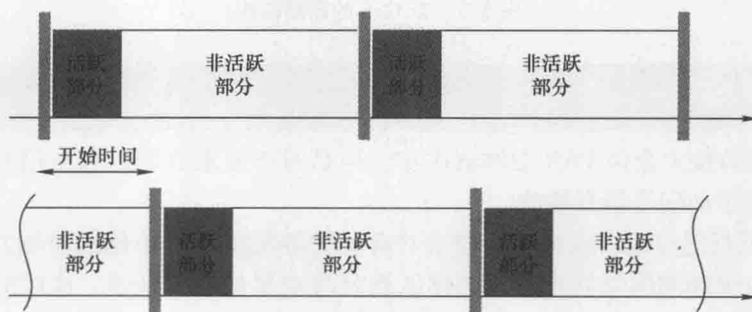


图 5-7 多跳网络中的超帧结构

5.4 MAC 层数据传输模型

无线频谱共享的特性给无线通信系统设计人员制造了一些挑战。IEEE 802.15.4 标准的 MAC 层考虑到了这些挑战，并提供了一些措施（带确认的 CSMA－CA机制和帧完整性校验）以提高通信的可靠性。

IEEE 802.15.4 标准的数据传输模型取决于网络拓扑结构。在星形网络中，数

据通信始终发生在 PAN 协调器和网络设备之间。但是，在对等网络中，网络设备可与自己所属的协调器或其附近的任何网络设备通信。

依据 PAN 协调器是否是信标使能的，星形网络可以有两种类型的数据传输机制：发送给 PAN 协调器的数据传输和来自于 PAN 协调器的数据传输。此外，对等网络支持点对点的数据传输。

5.4.1 到协调器的数据传输

在信标使能的网络中，欲发送数据给协调器的网络设备需与协调器周期性发出的信标帧同步。如果此网络设备是星形网络的一部分且有一个已分配的保障时隙（GTS），它将等待，直到超帧中分配给自己保障时隙时，发送数据给协调器，而不用时隙 CSMA。否则，此网络设备在超帧中的竞争访问周期，使用时隙 CSMA - CA机制来发送数据给协调器。协调器在接收到该数据帧后，如果要求，该协调器将会发送一个确认帧给网络设备，表示数据传输已经完成。此过程的报文序列图如图 5-8 所示。IEEE 802.15.4 标准将此过程称为“直接数据传输（direct data transfer）”。

在非信标使能的网络中，欲发送数据给协调器的网络设备首先采用 CSMA 机制来检查可用信道。如果信道空闲，该网络设备则将报文发送给协调器。如果要求确认，协调器通过发送一个确认报文给网络设备来表明其已经成功接收到数据帧。此过程的报文序列图如图 5-9 所示。

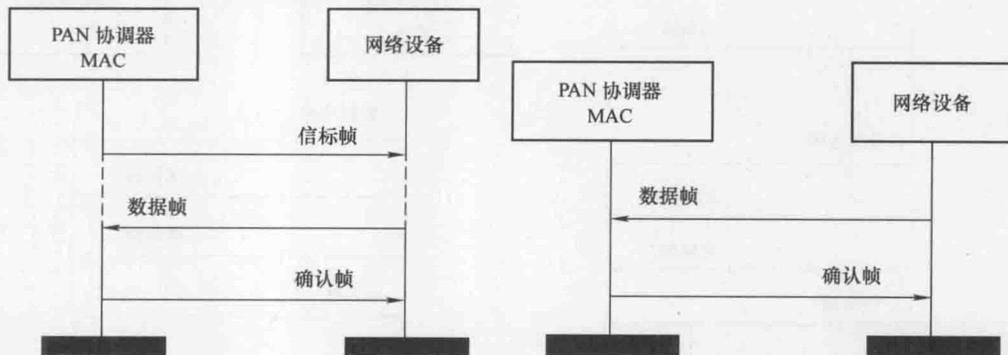


图 5-8 到协调器的数据传输——信标使能网络 图 5-9 到协调器的数据传输——非信标使能网络

5.4.2 来自于协调器的数据传输

当协调器有数据要发送给网络设备时，它不会立刻发出该报文；相反，它将该网络设备的短地址附加到自己信标帧中的某个特殊字段，即等待地址列表。这表示协调器有数据准备发送给这个网络设备。当网络设备接收到该信标帧并检测到协调器有数据准备发送自己后，网络设备会在超帧中的竞争访问周期（CAP）

发送一个 MAC 层的数据请求命令帧给该协调器。协调器在收到该数据请求命令帧后，发送一个确认帧对该命令帧进行确认，然后再将待定的数据帧发送给该网络设备。然后，网络设备给协调器发送一个确认帧来表明已经成功地接收到协调器发给自己的数据帧，这样本次通信便完成了。如果协调器有另外的数据要发送给同一个网络设备，协调器将在下一个超帧的信标帧中标明。IEEE 802.15.4 标准将此过程称为"间接数据传输（indirect data transfer）"，此过程的报文序列图如图 5-10所示。

为了简化实现，IEEE 802.15.4 标准的制定工作组决定不将确认帧和数据帧合并在一起。

间接数据传输也被协调器用来在非信标使能的网络中发送数据给网络设备。然而，协调器不能利用信标帧来标明等待发送给网络设备的报文，所以网络设备需要频繁地轮询协调器来查询等待的报文。IEEE 802.15.4 标准的 MAC 子层提供了一个机制来让更高层轮询报文。图 5-11 显示了在非信标使能的网络中的间接数据传输过程。当网络设备的较高层指示 MAC 层轮询等待的报文时，网络设备的 MAC 层发送一个数据请求命令帧给协调器，用来确认成功接收到了带确认帧的命令。随后，协调器将等待的报文发送给该网络设备。网络设备接收到该数据报文后，反馈一个确认帧给协调器。至此，本次数据通信完成。

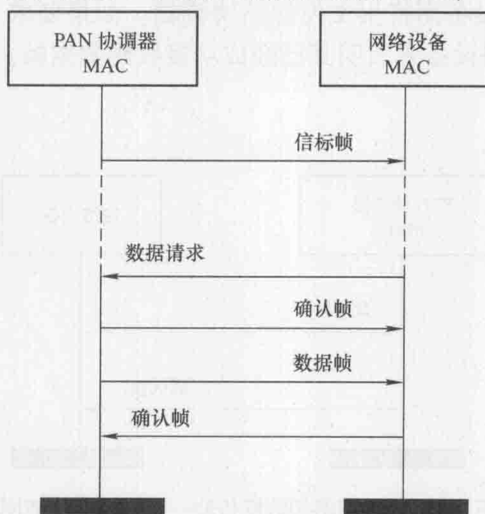


图 5-10　来自于协调器的数据传输——信标使能网络

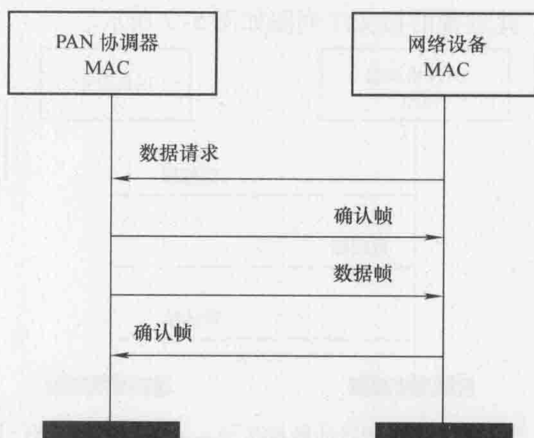


图 5-11　来自于协调器的数据传输——非信标使能网络

5.4.3　对等网络数据传输

对于对等网络拓扑结构，数据传输模式取决于管理无线网络的特定网络层。网络设备可能会保持处于接收模式，并扫描信道以获得发给自己的数据报；或者

可能周期性地发送信标帧来和其他潜在的处于侦听状态的网络设备实现同步。

5.5 MAC层服务

MAC子层为较高层提供两项服务：MAC层数据传输和MAC层管理服务（被称为MAC子层管理实体或MLME）。它们分别通过MAC层公用部分子层服务接入点（MCPS-SAP）和MAC层管理服务接入点（MLME-SAP）访问。对于这两种服务，IEEE 802.15.4标准定义了一系列协议原语来使能LR-WPAN设备的所有功能。图5-12详细地描述了IEEE 802.15.4协议栈体系架构和MAC层对等实体间的虚拟链接。

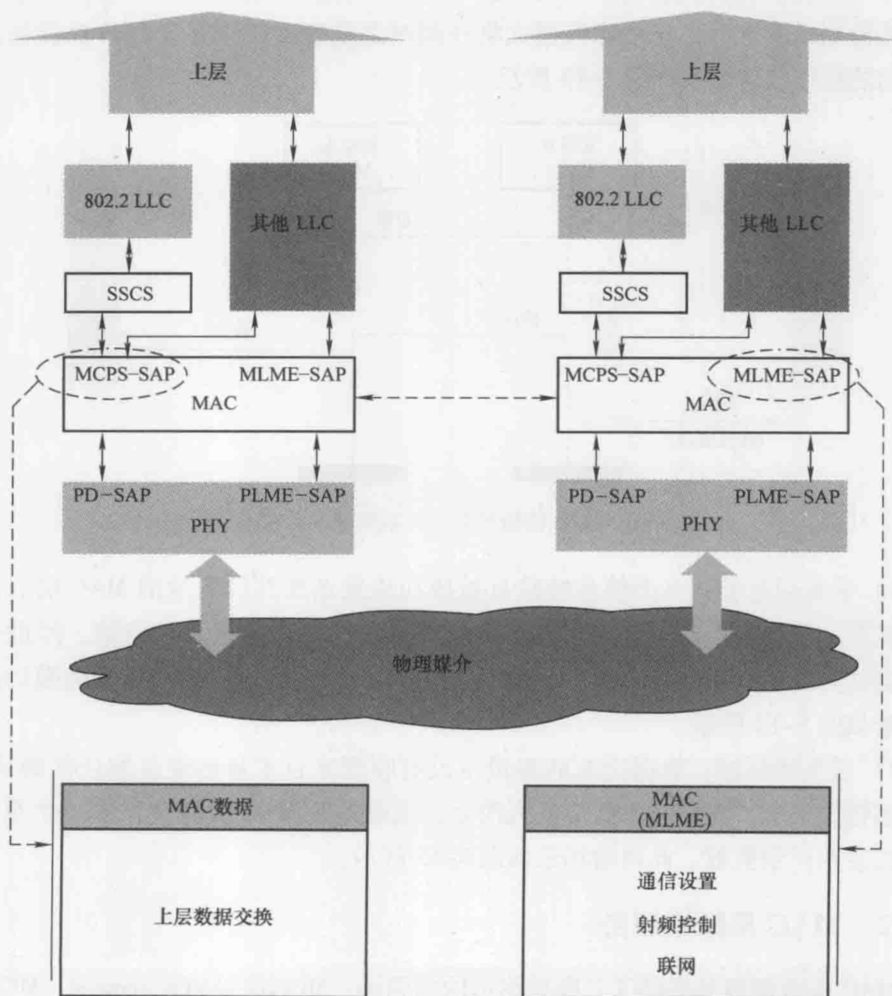


图5-12 IEEE 802.15.4标准协议栈体系结构

一个层的服务是其为更高层提供服务的能力。上层的功能是建立在较低层的服务之上的。MAC 层服务允许在对等实体之间传输协议数据单元。

5.5.1 传输场景

由于受无线通信介质的固有特性的影响，两个收发器之间的分组交换容易发生错误。当某个报文发生一个或多个错误时，该报文将不会被送达到期望的 MAC 层收件实体，或者是因为收件方的 PHY 层拒绝接收该报文；或者是因为接收方的 PHY 层无法与该报文同步（关联），该 PHY 此时是听不到该报文的。

任何带确认的数据交互都有以下三种可能的场景：

1）成功的数据传输：源设备发送一个报文到接收设备的 MAC 层。该报文被接收并检测无误之后，一个确认报文将在超时之前被接收设备发回给源设备。一例成功的数据传输场景如图 5-13 所示。

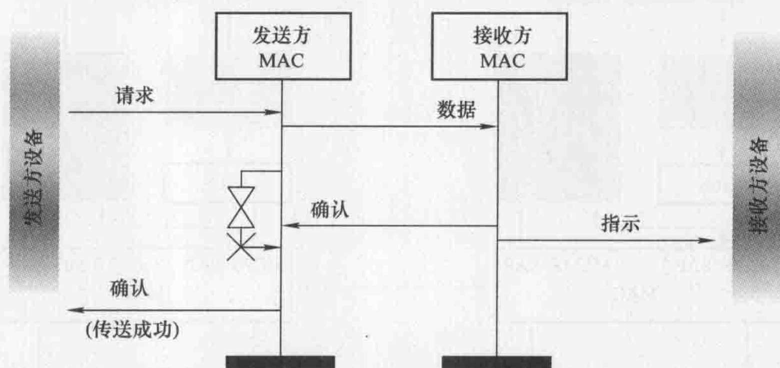


图 5-13　传输场景——数据成功传输

2）丢失信息帧：一个信息帧没有被成功地发送到其目的地的 MAC 层。在这种情况下，源设备会有一个超时的声明，然后尝试再次发送该信息帧。经过一系列的尝试失败后，源设备的 MAC 层会发送一个通知到其上层表明传输失败。此传输场景如图 5-14 所示。

3）丢失确认帧：数据交互的源设备没有收到来自于目的设备的任何确认帧。与前面情况类似，在一连串的尝试失败后，源设备的 MAC 层将会发送一个通知到其上层表明传输失败。此传输场景如图 5-15 所示。

5.5.2 MAC 层数据服务

MAC 层数据服务提供了三种数据传输的原语：MCPS – DATA. request，MCPS – DATA. confirm 和 MCPS – DATA. indication，如图 5-16 所示。该序列图显示了两个

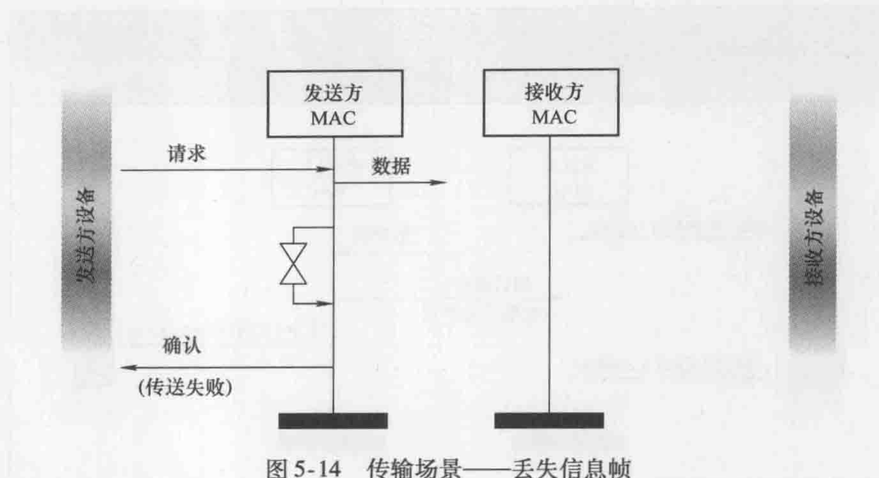


图5-14 传输场景——丢失信息帧

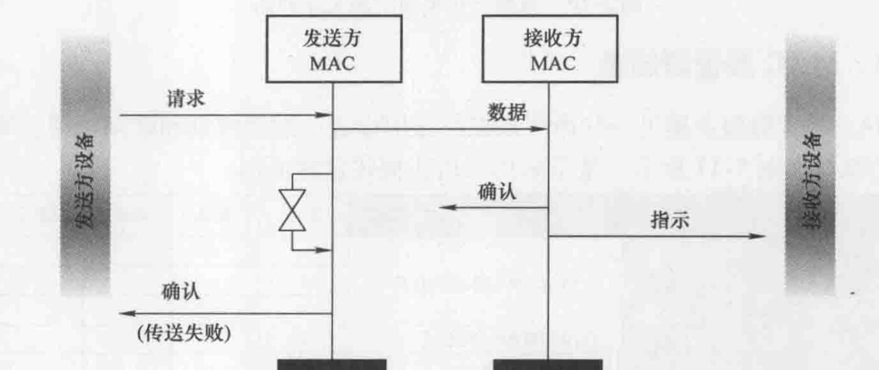


图5-15 传输场景——丢失确认帧

设备间的一次典型数据传输。数据服务要求对方MAC层发送响应，所以响应原语是不需要的。

由MAC数据服务提供的接口可以处理不同的寻址方案，使得星形网络和对等网络的实现简单。在这个意义上说，MAC层能使其上层决定在发送的分组中采用哪种地址类型，从而允许形成不同类型的网络（包括多跳Ad Hoc网络）。IEEE 802.15.4标准使用一个标准的64位IEEE地址和一个由一种相关机制分配出的短地址。此外，MAC层数据服务支持两个可选的原语，来使上层可以从MAC队列中清除一个MSDU。这两个原语分别是MCPS-PURGE.request和MCPS-PURGE.confirm，它们用于间接数据传输。例如，这两个原语可被用于当接收方设备在有机会从协调器重新获得某个等待的数据帧之前该数据帧中的信息就过期了的情景。

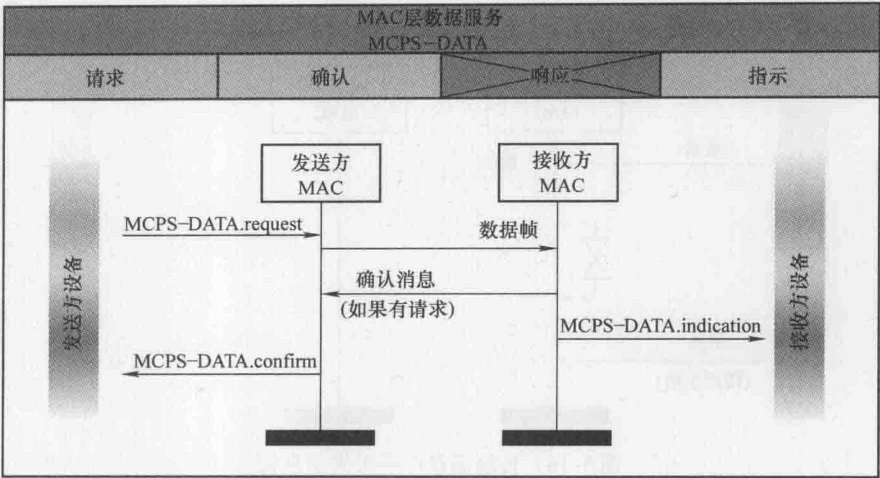


图 5-16　数据交换机制中报文序列图

5.5.3　MAC 层管理服务

MAC 层管理服务提供一些命令来控制通信设置、射频控制和联网功能。MLME 原语的归纳如图 5-17 所示。接下来的段落将概述这些原语。

原语	种类	描述	请求	确认	响应	指示
GET	通信设置	MAC PAN管理信息库	×	×		
SET			×	×		
RESET			×	×		
RX ENABLE	射频控制	启用和禁用射频系统	×	×		
SCAN		扫描射频信道	×	×		
ASSOCIATE	联网	与网络协调器的关联控制	×	×	×	×
DISASSOCIATE			×	×		×
GTS		GTS管理	×	×		×
ORPHAN		孤点设备管理			×	×
SYNC		与网络协调器的设备同步控制	×	×		
SYNC LOSS						×
START		信标帧管理	×	×		
BEACON-NOTIFY						×
POLL		无信标帧的同步	×	×		
COMM-STATUS		通信状态				×

图 5-17　MAC 层管理服务原语

为了能够实现非常低复杂度的设备，一些 MAC 层管理原语是可选的（即符合 IEEE 802.15.4 标准的设备可以不需要实现它们）。这些原语有 MLME - GTS、MLME - RX - ENABLE 和 MLME - SYNC。此外，其他原语仅对 RFD 是可选的，这些原语包括 MLME - ASSOCIATE.indication、MLME - ASSOCIATE.response、MLME - ORPHAN 和 MLME - START。

5.6 MAC 层 PAN 信息库管理原语

MAC 层 PAN 信息库（PIB）包含一些用于管理 MAC 子层的可配置属性。MLME – GET 原语和 MLME – SET 原语分别被用于读取和写入这些属性。此外，MLME – Reset 原语可被用来将这些属性复位成它们的默认值。MLME – Reset 原语也可以复位 MAC 子层和收发器的状态。图 5-18 所示为读取或写入 PAN 信息库（PIB）过程的报文序列图。

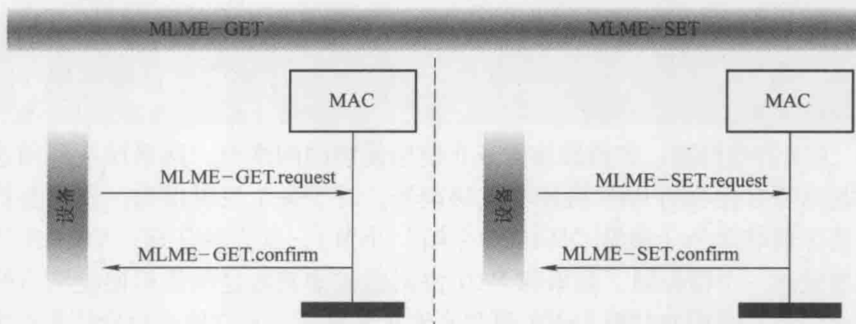


图 5-18 MAC 层 PIB 读写中的报文序列图

5.7 启用和禁用接收器

MLME – RX – ENABLE 原语可用来启用或禁用无线电接收器。该动作可被设置为立即执行或调度成在某个时刻执行。调度的目的是为了使 MAC 为较高层提供网络同步功能。设备的网络层可以通过调用该原语来利用该功能，例如调度在某个确定的时刻进行数据交换，从而降低系统的功耗。图 5-19 显示了这种原语的报文序列图。

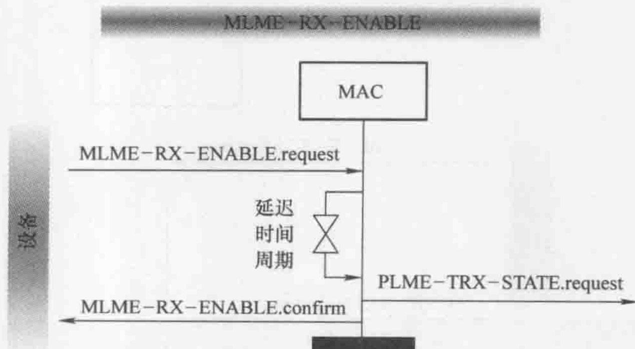


图 5-19 使能接收方的报文序列图

5.8　扫描射频信道

MLME - SCAN 允许发起对一个可用信道列表的扫描。信道扫描有以下有 4 种类型：

1）能量探测扫描：此扫描允许在每个指定逻辑信道测量无线电信号的能量。MLME 通过调用 PLME - ED. request 原语来执行该测量。PAN 协调器可采用这种方法来搜寻一个适合的信道以形成一个新的网络。

信标帧不仅由 PAN 协调器发送出。某个 PAN 网络中被配置为协调器的 FFD，可以通过广播信标帧来向其他设备表示自己的存在，同时为了其他设备的同步或有助于设备发现。

2）主动信道扫描：在信标使能或非信标使能的网络中，网络设备利用这种扫描来寻找出所有相邻的 PAN 协调器或协调器。对于每个逻辑信道，该设备首先发送一个信标请求命令（参见“MAC 命令帧”小节），这会使任何一个 PAN 协调器或协调器发送一个信标帧。如果该 PAN 协调器或协调器是非信标使能网络的一部分，那么它们将采用非时隙 CSMA 机制来发送信标帧；若它们是信标使能网络的一部分，那么它们将在下一个预定的信标间隔来发送信标帧。

3）被动信道扫描：协调器利用这种扫描来搜索在射频范围内的属于信标使能网络的网络设备。被动扫描意味着信道只是被动地侦听而不发送信标请求命令。

4）孤点信道扫描：允许一个孤立设备（此设备已失去与其协调器的链接）执行扫描，从而找到一个协调器。此扫描是按照指定列表中逻辑信道进行搜索的。

图 5-20 中的报文序列图显示了射频扫描的通用过程。扫描时间是 MAC 层停留在某个特定信道上的持续时间。该时间是基于最小超帧的大小，且用来自于上层的原语中的参数计算出来的。

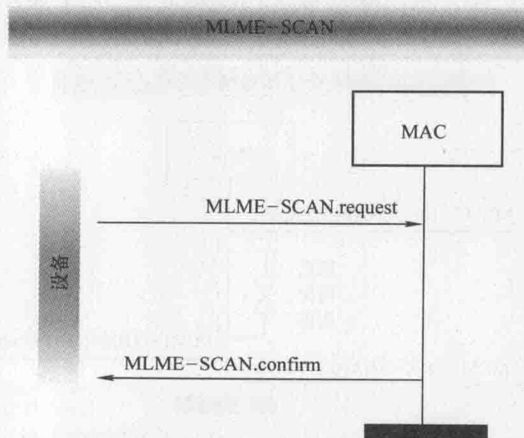


图 5-20　信道扫描机制中的报文序列图

当设备确定其已经失去与协调器的通信时，该设备就成为了一个孤点。通信丢失可能有很多原因，其中包括：

1）现有信道上的衰落或干扰。

2）由于现有信道的恶化，协调器切换到其他信道。

3）网络设备或协调器的移动，从而使二者离开了彼此的通信范围。

5.9 关联和取消关联控制

当前没有与任何网络相关联的网络设备，可以使用信道扫描程序来发现潜在的候选网络。如果设备希望加入信标使能网络，那么它使用被动扫描的方式；如果它试图加入一个非信标使能网络，那么它使用主动扫描的方式。在主动或者被动扫描成功后，从信标帧中获取到的所有信息都将传递到更高层；更高层将会选择一个合适的协调器加入其网络。如果设备正在试图加入一个信标使能网络，那么它首先要与选择加入的协调器发出的信标帧同步。这个过程由 MLME - SYNC. request 原语完成（参见 5. 12 节同步控制）。一旦同步，设备的较高层将会发出一个 MLME - ASSOCIATE. request 原语给 MAC 子层。在非信标使能网络中，设备不需要同步，设备的较高层不需要首先同步而可以直接发出关联请求。

IEEE 802. 15. 4 标准没有规定在信道扫描之后如何选择一个 PAN 协调器的详细过程。

请求关联的设备的 MAC 层收到关联请求原语后，发送一个关联请求命令给选定的协调器。当该协调器收到该命令后，该协调器回复一个确认帧给该设备。值得注意的是确认帧对于数据帧是可选的，但是在该过程中是要求的。对该报文的确认并不意味着该关联已经被接受，而仅仅是确认收到了该命令请求。PAN 协调器的 MAC 层在接收到该关联请求后，需要确定自己是否有足够的资源以允许另外一个设备在自己的网络中。PAN 协调器在 macResponseWaitTime（一个 MAC 常量参数）规定的时间内做出决定，否则发出请求的设备将宣布超时。

依据自身的能力和应用的需求，协调器可以通过发出一个带有合适参数的 MLME - ASSOCIATE. response 来接受或拒绝该关联请求。协调器通过使用“间接数据传输”（参见 5. 4. 2 节来自于协调器的数据传输）来将关联响应原语发送给请求关联的设备。如果协调器是信标使能网络的一部分，协调器在其信标帧中表明一个报文正在等待发送给入网设备。如果该设备正在试图加入一个非信标使能网络，那么该设备在请求来自于协调器的响应之前等待 macResponseWaitTime 时间。

关联过程的另一个重要特点是设备可能向 PAN 协调器请求一个 16 位的短地址。这能提高带宽的利用率，因为它减少了分组的总长度（16 位而不是 64 位的地址）。如果申请关联的设备不要求分配一个 16 位的短地址，那么该设备将使用自己的 64 位唯一的扩展地址来加入网络。图 5-21 显示了关联机制的报文序列图。

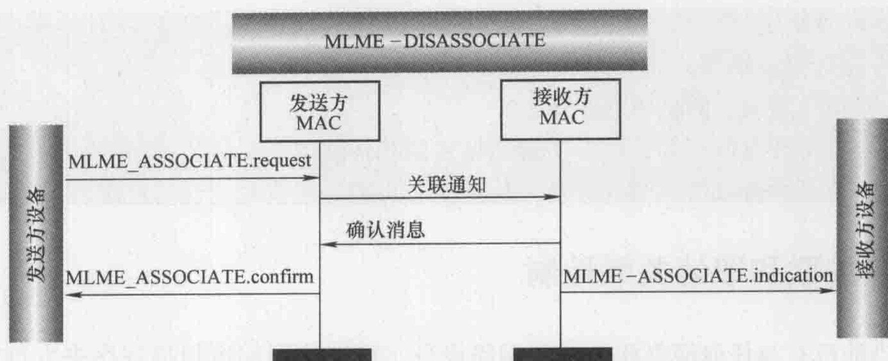


图 5-21　关联机制的报文序列图

网络设备或 PAN 协调器可以通过使用 MLME－DISASSOCIATE 原语来启动取消关联过程。网络设备或 PAN 协调器中的协议栈高层可以通过发布 MLME－DISASSOCIATE. request 原语给 MAC 子层来请求取消关联。然后，依据哪个设备发起取消关联请求，该设备的 MAC 子层通过“到协调器的数据传输”或“来自于协调器的数据传输”方式发送一个取消关联命令帧给相应的设备。此过程的报文序列图如图 5-22 所示。

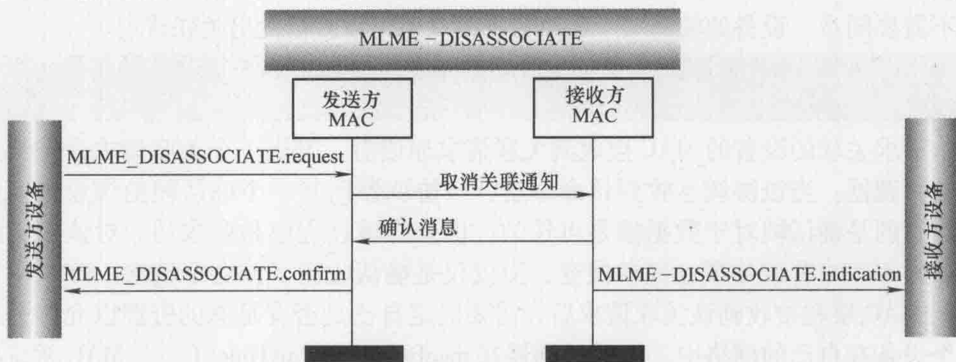


图 5-22　取消关联机制的报文序列图

5.10　保障时隙管理

如前所述，在 IEEE 802.15.4 标准中，超帧的使用是可选的，这样就让保障时隙的实现成为可能。MLME－GTS 原语允许分配一个新的 GTS，释放一个现有的 GTS，或者重新分配一个 GTS 以消除时隙碎片。对 GTS 的支持在 IEEE 802.15.4 标准 2006 修订版中是可选的。

一个 GTS 能扩展至一个或多个超帧时隙。GTS 的管理仅由 PAN 协调器执行，PAN 协调器控制着 16 个可用时隙中的多少个时隙被分配在非竞争周期（CFP），余下的时隙被分配在竞争周期。PAN 协调器可能分配最多 7 个 GTS。

可选的 GTS 能力允许 PAN 协调器与某个网络设备之间实现一个有保障网络吞吐量的无线链路（假设该链路是可靠的）。PAN 协调器完全可以分配一个 GTS 覆盖整个非竞争周期（CFP），而这个 CFP 又可能会占据整个超帧周期，即超帧周期长度减去 440 个字符的最小长度的竞争访问周期。

如图 5-23 中报文序列图所示，GTS 分配机制由该网络设备发起。如图 5-24 中报文序列图所示，GTS 释放机制可以由网络设备或 PAN 协调器发起。接收到一个 GTS 请求报文后，PAN 协调器根据超帧中竞争周期中剩余的时隙数和要求的时隙数来确定是否有足够的时隙来满足该 GTS 请求。

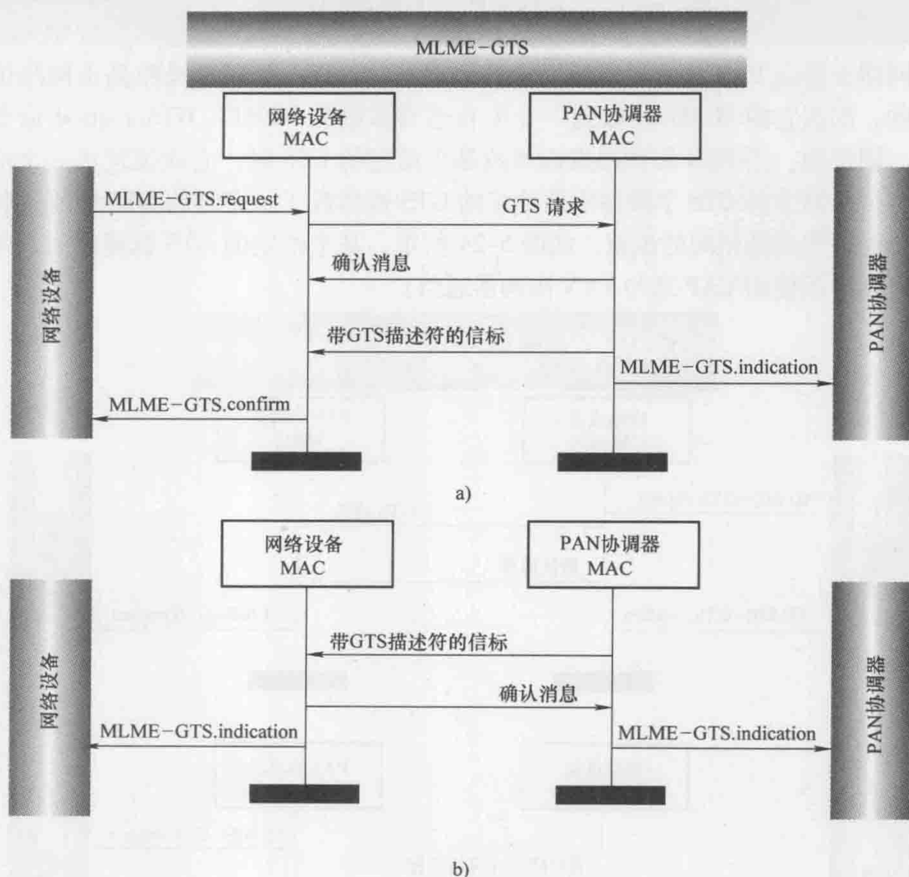


图 5-23　GTS 分配过程

a）网络设备发起　b）PAN 协调器发起

当 PAN 协调器响应某个 GTS 请求，它会产生一个信标帧，该信标帧中的 GTS 字段标明被分配的时隙以及数量。如果该超帧没有足够的空间来分配一个新的 GTS，那么 PAN 协调器将拒绝该请求。这时，信标帧中的 GTS 字段标明非竞争周期中剩余的时隙数目。

当一个网络设备在 GTS 使能的网络中产生一个数据请求时，该设备必须推迟传输直到分配的 GTS 开始。该传输不能占用多于分配的时间（分配的时隙数目）。

GTS 报文交换机制是完全需要确认的。该机制包括 MLME - GTS. confirm 原语的产生，该原语包括所有与 GTS 分配过程相关的信息。在被分配了一个 GTS 后，网络设备使用这个分配给自己的时隙来与 PAN 协调器通信，当然该网络设备也可以使用 CAP 来与 PAN 协调器通信。

网络设备在某个 GTS 中的传输不需要使用 CSMA - CA。分配的保障时隙是有方向性的，即数据传输可以是从网络设备到 PAN 协调器或从 PAN 协调器到该网络设备。

网络设备或 PAN 协调器可以请求释放现有的 GTS。如果该操作是由网络设备发起的，那么它的 MLME 应收到一个带有适当参数的 MLME - GTS. request 命令的指示。同样的，当 PAN 协调器发起释放某个给定的 GTS 时，它应该发送一个信标帧，该信标帧中的 GTS 字段标明该给定的 GTS 被释放了。完整的 GTS 释放过程与 GTS 分配过程遵循相同的步骤，如图 5-24 所示。某个给定的 GTS 被释放后，网络设备可以继续使用 CAP 来与 PAN 协调器通信。

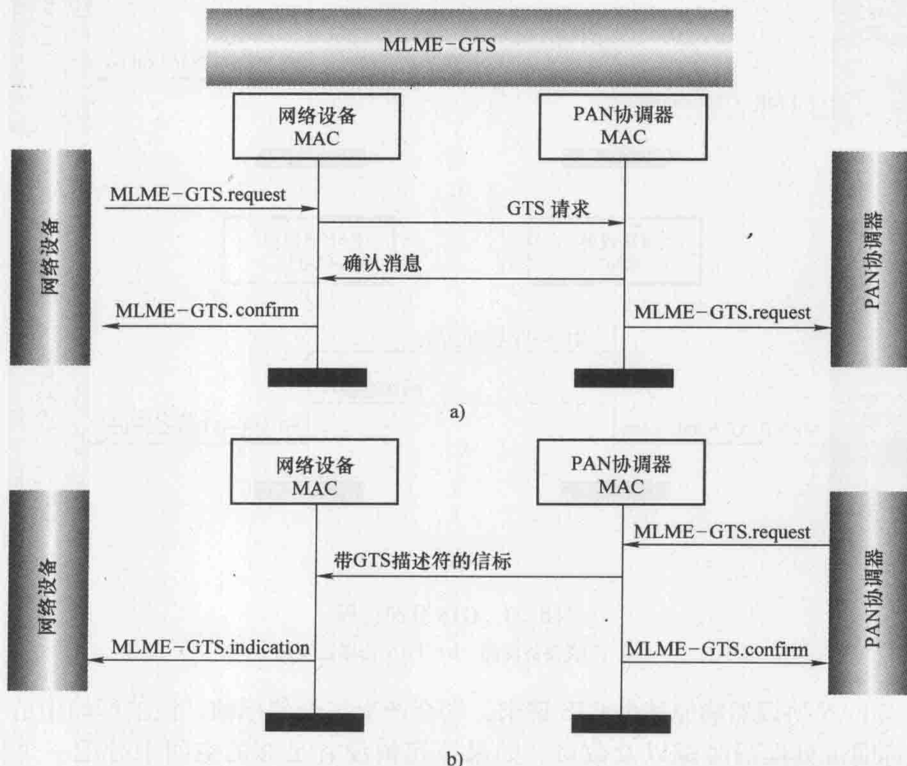


图 5-24　GTS 释放过程

a）网络设备发起　b）PAN 协调器发起

在一个 GTS 使能的网络中，超帧的非竞争周期可能会由于时隙的几次分配和释放而变成片断的。PAN 协调器负责移去非竞争周期中的这些间隙以确保带宽的最佳利用。

如果某个设备失去与 PAN 协调的同步，分配给该设备的 GTS 将被释放掉。该设备在与 PAN 协调器（在一个扫描过程后）重新建立连接后，可以再次要求分配 GTS。

5.11　孤点设备管理

当某个网络设备失去与 PAN 协调器联系时，该设备使用 MLME - SCAN 原语来执行一次独立的信道扫描。作为这种信道扫描的一部分，网络设备的 MAC 层在每个可用的和规定的信道上发送孤点通知命令报文。当 PAN 协调器或某个协调器的 MAC 层接收到这个通知，它将会产生一个 MLME - ORPHAN. indication 原语，从而让自己来验证该网络设备是否属于自己的网络。如果该网络设备与自己有关，那么它产生一个 MLME - ORPHAN. response 原语。此时，该协调器的 MAC 层将发送一个协调器调整命令。如果该网络设备与自己无关，那么它将不做出响应。图5-25 显示了一个孤点通知机制的报文序列图。

精简功能设备（RFD）不要求实现 MLME - ORPHAN 原语。

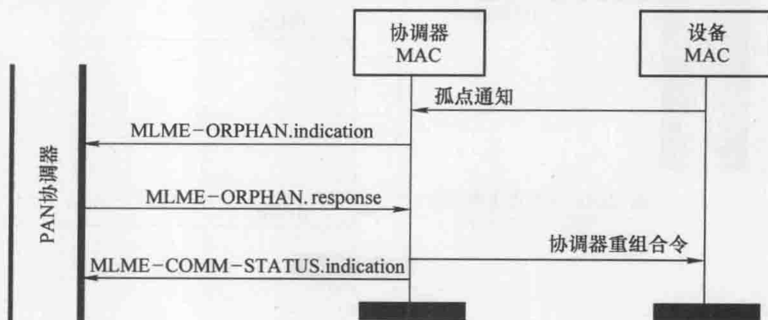


图 5-25　孤点通知机制的报文序列图

5.12　同步控制

MLME - SYNC 和 MLME - SYNC - LOSS 原语被用来实现与协调器的同步控制。MLME - SYNC 允许在信标使能 PAN 中的网络设备定位和跟踪信标帧。该搜索过程由 MLME - SYNC. request 原语发起。激活无线电接收机并等待一段给定的时间以接收到来自于某个协调器的信标帧，此时该搜索完成。

在一个信标使能网络中，信标帧的搜索可以通过以下两种方式中的一种来实

现：①网络设备的 MAC 层持续地跟踪其协调器的信标帧；②网络设备的 MAC 层仅一次定位到其协调器的信标帧。在这两种方式中，如果某个接收到的信标帧中标明有等待的数据报发送给该网络设备，那么该网络设备发送一个数据请求命令给该 PAN 协调器。图 5-26 显示了网络设备同步的报文序列图。MLME - SYNC. request 不被用于非信标使能网络。

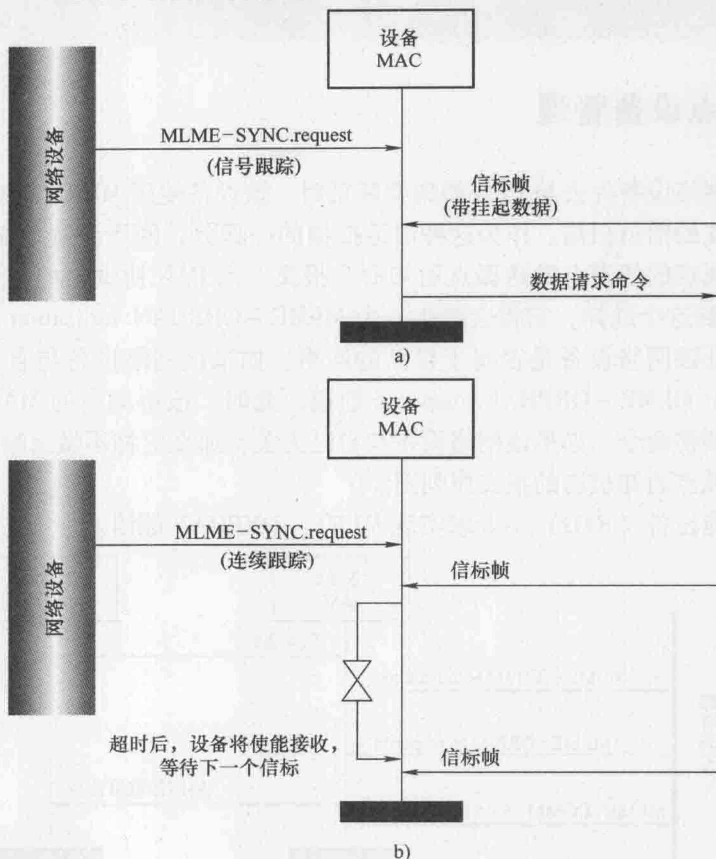


图 5-26　网络设备同步的报文序列图

a）单次跟踪　b）持续跟踪

在网络设备与协调器失去同步的情况下，该网络设备的 MAC 层产生一个 MLME - SYNC - LOSS. indication 原语。以下四种情况可能会导致失去同步：

1）信标帧丢失：在 MLME - SYNC 之后，无论是在最初或在跟踪过程中，信标帧都没有被接收到。图 5-27 描述了这种情况的报文序列图。

2）协调器丢失：几次试图与协调器通信失败。

3）PANID 冲突：网络设备检测到一个 PAN ID 冲突，即在该网络设备的通信范围内有两个不同的 PAN 协调器具有相同的 ID。

4）调整：网络设备从 PAN 协调器接收到一个协调器调整命令报文。

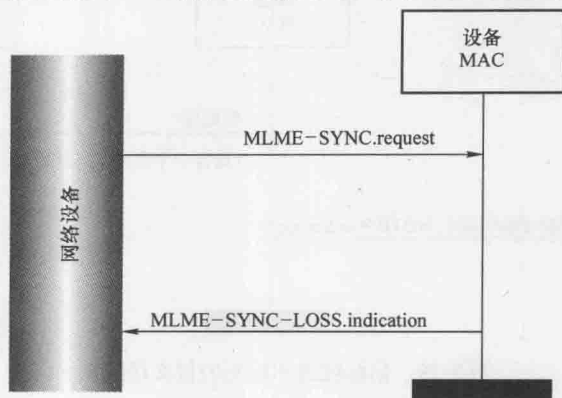


图 5-27　由于信标丢失而失去同步对应的报文序列图

5.13　信标帧管理

MLME - START 原语被用来初始化信标帧的产生。该原语的参数允许配置某个网络设备为 PAN 协调器或协调器，选择某个逻辑信道、建立信标帧的周期和设置超帧的特性。在 MLME - START. request 原语后，该设备的 MAC 层将用 MLME - START. confirm 原语进行响应，如图 5-28 所示。当某个网络设备接收到一个信标帧，并且该信标帧包含了自己所属网络的 PAN ID，那么该设备的 MAC 层将解译该信标帧的内容。如果该信标帧包含一个或多个字节的载荷（数据），那么该设备的 MAC 层将发出一个 MLME - BEACON - NOTIFY. indication 原语。图 5-29 描述了该信标帧通知机制。

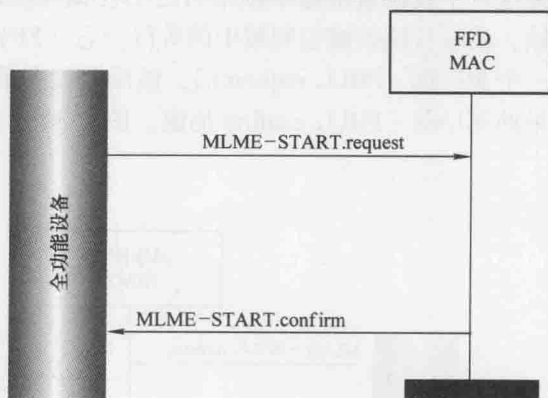


图 5-28　开始产生信标帧传输的报文序列图

在对等网络中的全功能设备（FFD）可以产生信标帧并发送给其周边设备。这些信标帧在网络形成的过程中可以作为 Hello 报文。如果 MLME - START 原语中的 PANCoordnator 参数被设置为假（FALSE），那么这个产生信标帧的网络设备被称为协调器。在 IEEE 802. 15. 4 标准中，仅全功能设备（FFD）可以成为协调器和有产生信标帧的能力。

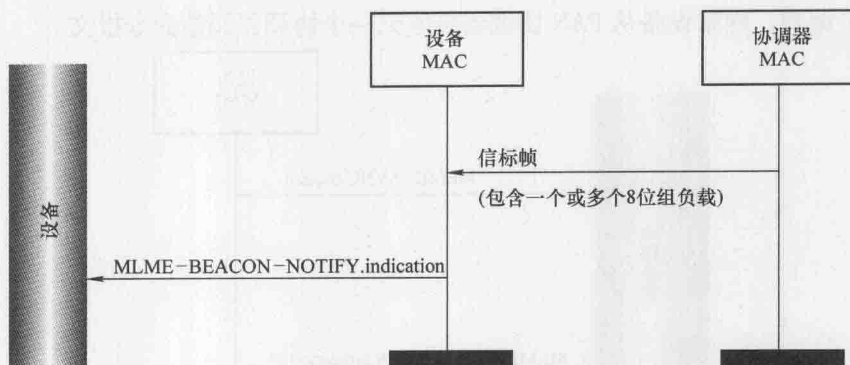


图 5-29　信标帧通知机制的报文序列图

5.14　无信标帧同步

对于非信标使能网络，网络设备可以使用 MLME - POLL 原语来轮询协调器中的待发数据。当网络设备的 MAC 子层接收到一个 MLME - POLL. request 原语时，它发送一个数据请求命令帧给自己的协调器。该协调器会发给该网络设备一个响应帧，该响应帧的帧控制域中的等待标志（FP）标明是否有待发给该设备的数据。在一个 MLME - POLL. request 后，该网络设备的 MAC 层将产生一个带有此次轮询结果的 MLME - POLL. confirm 原语。图 5-30 显示了该原语的报文序列图。

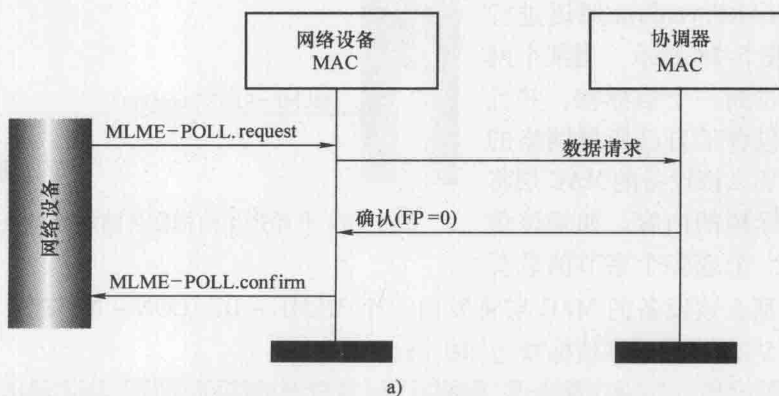
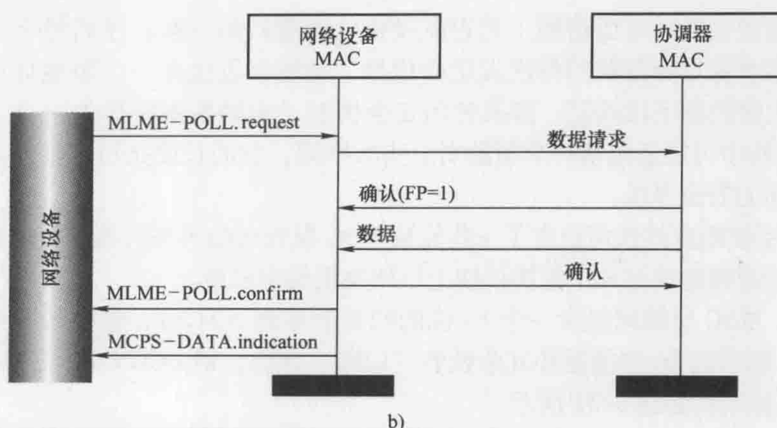


图 5-30　轮询协调器的报文序列图

a）无待发数据



b)

图 5-30　轮询协调器的报文序列图（续）

b）有无待发数据

如果网络设备接收到其协调器发出的信标帧，那么该网络设备的 MAC 层将检查该信标帧中的地址列表字段。如果自己的地址在该列表中，那么该网络设备的 MAC 层给该协调器发送一个数据请求报文，如 5.4.2 节“来自于协调器的数据传输”小节所述（信标使能）。

5.15　通信状态

利用 MLME - COMM - STATUS. indication 原语，网络设备的 MAC 层可以给其上层产生各种通信状态的报文。该原语在下述情况发生时被调用：

1）在由一个响应原语引起的传输之后。

2）在接收到的报文没有通过安全检测之后。

IEEE 802.15.4—2006 标准的不同修订版增加了一些 MAC 层功能。增加的功能用于支持 PHY 层的一些特定的限制，以符合一些不同地域的不同要求（例如，运行于 950MHz 的日本频段，或 IEEE 802.15.4a 标准的修订版增加了额外的功能以支持位置感知能力。

5.16　MAC 层帧结构

IEEE 802.15.4 标准的 MAC 层帧结构被设计得简单和灵活，同时具备最少的要素以克服无线传输的挑战。MAC 层帧由三个部分组成：帧头、长度可变的有效载荷和帧尾。

MAC 层帧头中包含一个帧控制字段，一个序列号字段，一个地址字段和可选的辅助安全头部字段。帧控制字段规定了帧类型、安全机制、地址字段的格式和

内容。帧控制字段同时还指明了是否需要接收者返回确认帧。序列号字段包含一个数目，这个数目随着帧的每次发送而递增。地址字段包含一个源地址或目的地址，具体由帧控制字段规定。如果启用安全机制（由帧控制字段的一个子字段决定），帧结构中可能还包括一个辅助安全头部字段，它的长度是可变的，具体长度取决于采用的安全等级。

MAC 层帧的有效载荷包含了一些能被 MAC 层处理的事务类型的特定信息，这些信息能被逻辑地放在几个被协议栈上层所使用的字段里。

最后，MAC 层帧尾包含一个 16 位的帧校验序列（FCS），该帧校验序列是基于 ITU－T 标准的 16 位的循环冗余校验（CRC）算法，即 CCITT 16 位 CRC。通用的 MAC 层帧结构如图 5-31 所示。

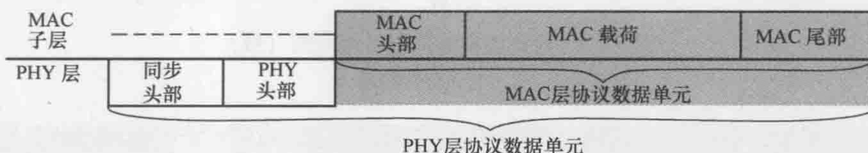


图 5-31　通用的 MAC 层帧结构

当 MAC 层帧的三个组成部分封装到物理层（PHY）分组时，它被称为 MAC 层协议数据单元（MPDU）。

IEEE 802.15.4 标准定义了四种类型的 MAC 层帧：信标帧、数据帧、确认帧和 MAC 命令帧。这些帧由接下来的段落所描述。

5.16.1　信标帧

在信标使能网络中，一个全功能设备（FFD）可以发送信标帧。在一个信标帧中，地址字段包含源 PAN ID 和源设备地址。信标帧的 MAC 层有效载荷可以分为四个字段：

1）超帧定义字段：包含一些定义超帧结构的参数（如果存在的话）。

2）待发的地址定义字段：包含地址列表字段中列出的地址的数量和类型。

3）地址列表字段：包含一个协调器的待发数据的目标设备地址的列表。

4）信标帧载荷字段：可被高层使用的可选字段。例如，该字段可用于在覆盖范围内向所有加入网络的设备广播数据。

信标帧的格式如图 5-32 所示。

MAC帧头				MAC载荷				MAC帧尾
帧控制	序列号	地址字段	辅助安全头部	超帧规格	GTS字段	等待的地址字段	信标帧载荷	FCS

图 5-32　信标帧的格式

5.16.2　数据帧

数据帧是 MAC 子层用来传输数据的。其地址字段包含源设备和/或目的设备的 PAN ID 和设备 ID，如 MCPS - DATA. request 原语规定。数据帧的格式如图 5-33 所示。

MAC帧头				MAC载荷	MAC帧尾
帧控制	序列号	地址字段	辅助安全头部	数据载荷	FCS

图 5-33　数据帧的格式

5.16.3　确认帧

确认帧是由 MAC 子层发出用来向发送方确认已经接收到报文。只有当接收到的报文要求确认并且 FCS（帧校验序列）计算正确时，接收设备才会生成确认帧。

确认帧不包含 MAC 层帧头中的地址字段，同样也不包含 MAC 层帧的有效载荷。

当某个网络设备接收一个确认帧时，它首先验证该确认帧是否是其期望收到的，它会将接收到的确认帧序列号与期望收到的序列号进行匹配；如果不匹配，这个确认帧将会被丢弃。确认帧的格式如图 5-34 所示。

确认帧被设计得很短以尽量减少网络流量。回顾一下，当要求报文接收确认帧时，每一个 MAC 层帧都对应着要有一个确认帧。

MAC帧头		MAC载荷	MAC帧尾
帧控制	序列号	→	FCS

图 5-34　确认帧的格式

5.16.4　MAC 命令帧

MAC 命令帧由 MAC 子层发起，并负责管理所有 MAC 层的传输控制。表 5-1 列出了每个 MAC 命令的类型。

表 5-1　MAC 命令帧类型

命令标识符	命令类型
1	关联请求
2	关联响应
3	取消关联通知

（续）

命令标识符	命令类型
4	数据请求
5	PAN ID 冲突通知
6	孤点通知
7	信标帧请求
8	协调器重组
9	GTS 请求
10～225	保留

MAC 命令帧的 MAC 层有效载荷包含两个字段：MAC 命令类型和 MAC 命令有效载荷。MAC 命令有效载荷包含所用命令类型的特定信息。图 5-35 详细描述了 MAC 命令帧的格式。

MAC帧头				MAC载荷		MAC帧尾
帧控制	序列号	地址字段	辅助安全头部	命令类型	MAC命令载荷	FCS

图 5-35　MAC 命令帧的格式

5.17　MAC 功能场景

IEEE 802.15.4 标准包含一个详细的解释机制来定义 MAC 层的功能。以下各段简要概述了这些机制。

5.17.1　访问信道

在 IEEE 802.15.4 标准中，网络设备在试图发送任何帧之前都会采用 CSMA－CA 的方式来访问物理无线信道。例外的情况包括信标帧、GTS 传输、确认帧以及在数据请求命令帧之后的数据帧（如果 MAC 子层能在命令帧后 12～32 个符号内返回一个数据帧）。

在信标使能 PAN 中，MAC 子层将使用时隙的 CSMA－CA 算法；相反，在非信标使能 PAN 中，它将使用非时隙的 CSMA－CA 算法。

5.17.2　PAN 网络形成和维持

试图加入某个网络的网络设备，必须通过扫描在其可用的信道列表中的射频信道来定位这个网络。如前文所述，MLME－SCAN 原语允许采用主动和被动的信标扫描。在找到一个合适的协调器发出的信标帧之后，网络设备将启动关联过程。

与PAN协调器或者协调器失去通信的设备，将执行一个孤点扫描过程，扫描的信道是其自己的可用信道列表中罗列的信道。一旦协调器收到孤立设备的查询，协调器将会返回一个协调器重新调整命令。

在一个信道扫描之后，如果没有合适的网络加入，全功能设备可以通过使用MLME - START. request原语成为一个PAN协调器。在某些情况下，两个PAN协调器有可能配置了相同的PAN ID。造成这种问题的原因之一是一个PAN协调器在没查询相邻协调器的情况下就自我设置了PAN ID。

一个PAN协调器如果收到了从其他PAN协调器发出的与自己PAN ID相同的信标帧，或者从它的子设备那里接收到了PAN ID冲突通知的命令，那么该PAN协调器就检测到了PAN ID冲突。与此类似，当一个网络设备接收到一个与自己所属网络PAN ID相同的信标帧，并且此时不是正确的信标周期或者该信标帧携带的源设备地址与自己的PAN协调器不同，那么该设备就检测到了PAN ID冲突。

在PAN协调器检测到冲突之后，它会执行一个主动信道扫描来选择一个新的PAN ID。此后，它会向与其相关的网络设备广播一个协调器调整命令。

PAN协调器分配其PAN ID的过程不在IEEE 802.15.4标准规定范围之内。

5.17.3 设备同步

在信标使能网络中，设备需要与信标帧同步来检测任何待发的报文。在非信标使能的网络中，设备也需要发送充当“Hello”报文角色的信标帧来让周边的设备发现自己。

5.17.4 GTS管理

PAN协调器负责维持超帧结构的完整，控制保障时隙的分配、释放和再分配。

网络设备可以请求GTS覆盖几个超帧时隙。PAN协调器则根据非竞争周期（CFP）中的可用时隙数和整体网络的需求，来决定是否允许该请求。MCPS - DATA. request原语包含了一个参数，该参数用来标明该帧将被在GTS（保障时隙）中传输或者在竞争访问周期（CAP）中传输。当GTS传输被请求时，传输会被推迟直到被分配的GTS开始。

网络设备或PAN协调器都可以启动GTS释放。当协调器在信标帧中标明了任何对GTS分配的变更时，网络设备可以使用GTS请求命令。PAN协调器在由于之前GTS释放所引起的GTS碎片检测完成后，启动GTS再分配。

5.18 安全服务

IEEE 802.15.4标准的MAC层提供了由MAC PIB控制的安全服务。MAC子层提供了两种安全模式：无安全模式和安全模式。

为满足与安全模式相关的目标，IEEE 802. 15. 4 标准中 MAC 层的一个重要功能是帧安全。帧安全实际上是一组可能由 MAC 层向上层提供的可选服务。IEEE 802. 15. 4 标准力求在需要这些服务的诸多应用程序中找到一个平衡点，并尽量减少那些执行时不需要这些服务的应用的负担。以下各小节将介绍这些可用的服务。

由于针对的应用众多，所以 IEEE 802. 15. 4 标准没有定义认证和密钥交换过程。

5. 18. 1　数据保密性

数据保密性是使用对称密码进行加密的，使用相同的密钥在报文源加密明文和在报文目的地解密密文。没有密钥的设备不能解密报文。IEEE 802. 15. 4 标准定义了信标帧的有效载荷、命令帧的有效载荷以及数据帧的有效载荷的加密方法。其他报文，例如确认帧以及报文中的部分字段（比如地址）是不加密的。

5. 18. 2　数据真实性

数据的真实性，也被称为数据的完整性，它提供一种服务，该服务能使接收设备通过附加到报文中的消息完整性代码（MIC）来检测该报文是否受到了没有正确加密密钥的某方的篡改。该标准定义的消息完整性代码（MIC）校验的内容包括：MAC 层帧头、辅助安全头部、无安全模式下的数据帧有效载荷、信标帧和 MAC 命令帧。数据的完整性是基于 IEEE 802. 15. 4 标准的应用最常用到的一种安全服务。与文件传输或语音通信应用所采用的协议不同，基于 IEEE 802. 15. 4 标准的应用所传递的报文通常不包含秘密信息，其更关注的是报文是否是经过验证的（即报文的源端是已知的和受信任的），以及是否能检测出报文是否经过任何篡改或修改。例如，一幢大厦的灯被关掉的事实通常不是秘密；然而，更重要的是控制这个大厦关闭电灯的报文要来自于可信赖的源端（比如房间的开关），而不是来自于捣蛋鬼或者黑客。

为了避免 IEEE 802. 15. 4 标准的网络遭到重放攻击（这里的重放攻击指的是一条旧消息被没有加密密钥的恶意实体存储然后重播），数据认证服务在报文的辅助安全头部放置了一个序列号。当报文被接收时，接收方将该序列号的值与自己存储的值相比较；如果它比存储的值更新，那么重放保护检查通过，新值被存储。虽然重放保护可以确定一个报文比另一报文新，但这只是相对的比较，它并没有做出绝对时间的比较。使用数据认证服务需要额外的内存来存储现值，同时消息完整性代码也增加了发送的延迟。

IEEE 802. 15. 4 标准在两种安全模式中提供了这三个服务的组合，以满足广泛的应用需求。

IEEE 802. 15. 4 标准的安全性部分在 2006 版本中被简化和精简了。其结果是，安全模式不能向后兼容。但是，遵循 2003 年版本的和遵循 2006 年版本的设备之间仍有可能通过使用不安全的模式来相互通信。

5.18.3　无安全模式

无安全模式没有提供安全服务。此模式非常适合于某些注重执行成本和不需要安全或者安全可以通过其他方法取得的应用。这种应用类型的例子包括在公共场所的广告亭，或在一个很大的物理安全区中心的低功耗无线电机控制器（其控制信号在这个区域以外根本无法被检测到）。

5.18.4　安全模式

在安全模式下，设备可能会根据不同的安全级别提供两种安全服务：数据机密性和数据真实性。表 5-2 所示的是被定义的八个安全级别。无安全模式被定义为 0 级，这一级别与遵循 2003 版要求部署的设备兼容。

在安全模式下使用数据真实性时，重放保护总是提供的。

表 5-2　IEEE 802.15.4 标准的安全级别

安全等级	安全属性	数据机密性	数据真实性	重放保护
0	无	关闭	无	无
1	MIC - 32	关闭	MIC - 32	是
2	MIC - 64	关闭	MIC - 64	是
3	MIC - 128	关闭	MIC - 128	是
4	ENC	开启	无	无
5	ENC - MIC - 32	开启	MIC - 32	是
6	ENC - MIC - 64	开启	MIC - 64	是
7	ENC - MIC - 128	开启	MIC - 128	是

安全级别 1 ~7 级均采用了 AES - 128（基于 128 位密钥和块大小为 128 位的高级加密标准）的对称密钥加密算法［27］。

安全级别 1 ~3 级提供了数据认证服务和长度分别为 32、64 或者 128 位的完整性代码，从而提供数据真实性和重放保护。安全级别 4 级提供了数据机密性服务。安全级别 5 ~7 级使用 AES 来提供数据保密性和数据真实性（消息完整性代码分别为 32、64 或 128 位）。完整性代码的长度并不是指 AES 算法的长度，而是指实际发送的报文中占用的比特位数。

这套安全机制具有几个优点。一个主要的优点是所有安全等级都只采用了一种加密算法。其他替代方法需要额外的算法（例如，使用哈希算法用于完整性检查）来提供一个完整的多层次的安全解决方案。这将导致更复杂和更高代价的实现。特别是，通过巧妙地重复利用 AES 算法，AES - CCM* 模式能使一个简单的算法在一个很小的实现中提供更高的安全服务。CCM* 是扩展的操作模式下的密码块链接消息认证码计数器。AES - CCM* 模式的使用保留了与其他 IEEE 802 标准

（如 IEEE 802.11i 和 IEEE 802.15.3 标准草案）的兼容性。这不仅使这些标准能重复利用这种模式的电路和代码，还保证了更多的学者能更好地回顾和研究该安全算法的弱点。随着时间的推移，这种高水平的研究和分析会增加人们对该安全算法的信心。

第 6 章 网络功能——源设备到目标设备之间的报文传输

IEEE 802.15.4 支持多种网络拓扑结构，从星形网络到基于对等（Peer－to－Peer）通信的多种网络拓扑类型，包括网格形、树形、簇形以及簇树形网络。尽管网络层本身不在 IEEE 802.15.4 标准覆盖范围之内，但是本章描述了多个基于 IEEE 802.15.4 标准构建的网络案例，并包括与之相关的报文路由算法。此外，本章还概述了报文路由算法，以便具体描述基于 IEEE 802.15.4 标准的网络能够达到的性能，以及广泛的应用范围。

6.1 特征概述

IEEE 802.15.4 标准支持主从配置的星形网络，以及一般形式的对等（Peer－to－Peer）通信。对等通信可以被用于构建各种类型的网络。星形网络（见图 6-1），是单跳或双跳网络（例如，所有网络设备都在单个设备的通信范围之内）。对等网络，例如网格网络（见图 6-2）或者簇形网络（见图 6-3），可能是多跳网络，即传递报文的源设备与目标设备不在相互的信号覆盖范围之内，需要通过多个中继设备转播报文来实现两者之间的通信。IEEE 802.15.4 标准支持单跳和多跳通信连接。

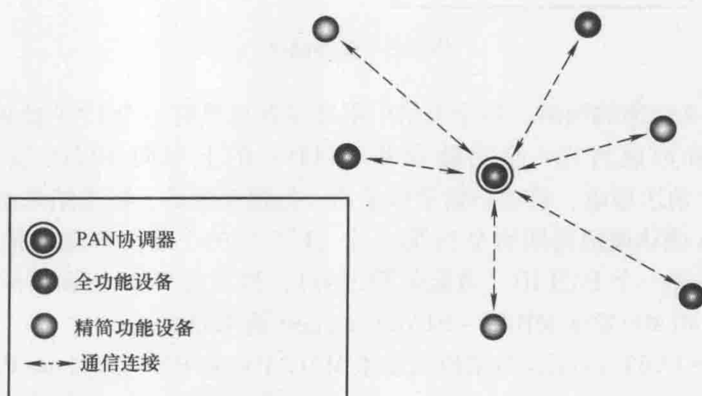


图 6-1 星形网络

正如第 5 章中描述的那样，当某个全功能设备成为 PAN 协调器之后，将启动

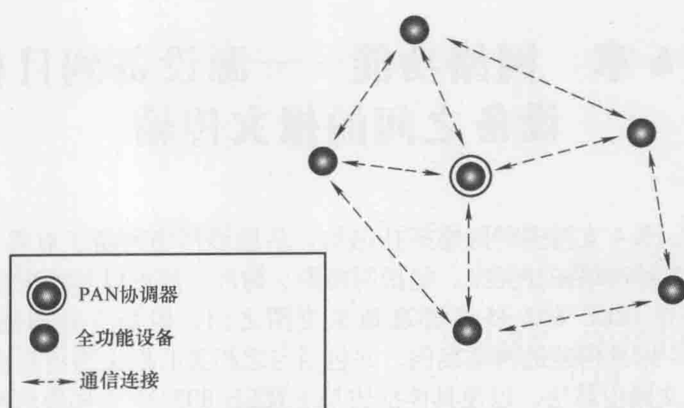


图 6-2　网格网络

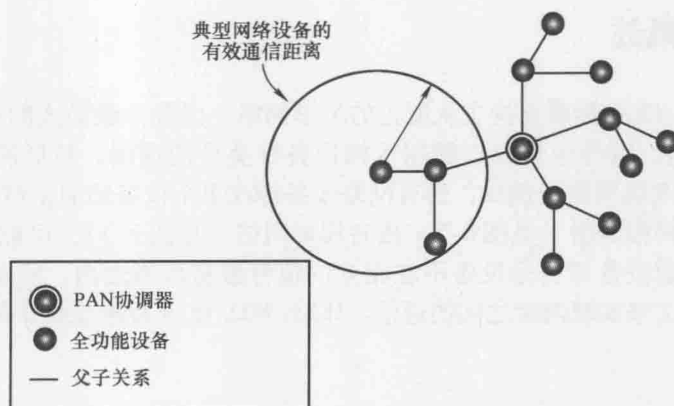


图 6-3　簇形网络

IEEE 802.15.4 标准的网络。每个网络中都必须有且只有一个 PAN 协调器。图 6-4 显示了网络的形成过程：全功能设备（FFD）的上层向 MLME 发送 MLME - SCAN.request 请求原语，请求扫描活跃信道。扫描完成后，扫描结果通过 MLME - SCAN.confirm 确认原语返回给全功能设备（FFD）的上层。如果扫描结果是可接受的，上层选择一个 PAN ID（可能是预定的），然后将 PAN 协调器的参数设置为 TRUE，并向 MLME 发送 MLME - START.request 请求原语。

MLME - START.request 请求原语要求 MAC 子层将 PAN ID 和 macPANId 值赋值到 MAC PIB 中，将逻辑信道 phyCurrentChannel 值放置到 PHY PIB 中。该过程完成后，MAC 子层向上层发送 MLME - START.confirm 确认原语，全功能设备作为 PAN 协调器开始工作，至此，网络开始启动了。

所有的 IEEE 802.15.4 设备都有一个唯一的 64 位 IEEE 地址——aExtendedAd-

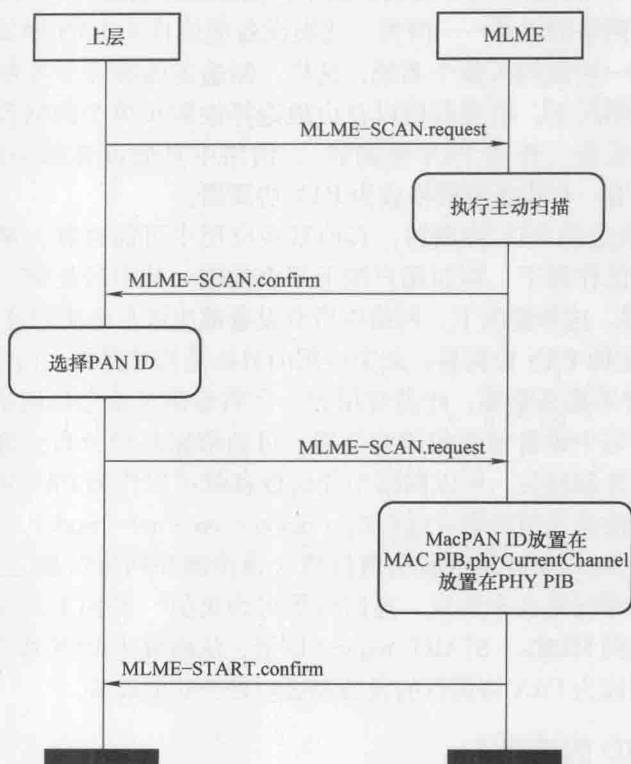


图6-4　网络的形成过程

dress，通常称为MAC层地址或物理层地址，该地址被存储在MAC PIB表中。设备在加入网络中时，通过自己的aExtendedAddress值来标识自己。在网络形成过程中，设备将此地址更换为PAN协调器提供的、更短的、特定网络的逻辑地址。

6.2　上层网络形成的策略与算法

正如第5章所述，一些与网络形成相关的策略和算法由协议栈的高层执行，并未在IEEE 802.15.4标准中定义。本章描述了其中的一些算法。请注意，这些算法只是理论上可行的算法，其他网络形成策略和算法在实际中也同样可用。

6.2.1　PAN协调器的选择

网络形成的第一步是选择PAN协调器。决定MLME-START.request请求原语（当PAN协调器参数设置为TRUE时）从高层传输至MAC层的策略，理所当然是由上层确定的。下面列举了多个应用的场景：

1）专用 PAN 协调器：某些应用场景中，例如某些家庭安全系统中，只有一个需要连接到外部网络的设备——网关。此类设备应该作为 PAN 协调器。这类应用通常要求消费者一次性购买整个系统，这样，制造者能够完全控制最终网络的设计和行为。其他情况下，消费者可以自由地选择性购买单个网络设备。此类网络仅有一个全功能设备（作为 PAN 协调器），网络中其他设备都是精简功能设备，即此类网络中只有一个设备有资格成为 PAN 协调器。

2）由事件决定的 PAN 协调器：其他某些应用中可能含有大量相同类型的设备，在外部激励的作用下，例如用户按下某个按钮，其中的任何一个设备都可能成为 PAN 协调器。这种情况下，网络中所有设备都应该是全功能设备。

3）自行决定的 PAN 协调器：此类应用的目标是构建网络，而网络中哪个设备是 PAN 协调器并不那么重要。此类应用的一个典型例子是定位网络。该网络的作用是确定网络中每个设备节点的相对位置，可能依据某种分布式算法来实现。此类应用可能没有外部网关，所以网络中任何设备都可以作为 PAN 协调器。构建此类网络的一种方法是采用网络带电形式（power - on - net - work），当设备启动后，设备的上层指示 MAC 层开始活跃信道扫描（该步骤在网络形成之前）。第一个完成信道扫描（如果网络尚未形成，返回结果将为负值）并向上层发送扫描结果的设备，将会接收到 MLME - START. request 原语，从而成为 PAN 协调器。像此前一样，所有有可能成为 PAN 协调器的设备都必须是全功能设备。

6.2.2　PAN ID 的选择

完成信道扫描后，扫描结果返回到设备中协议栈的上层。协议栈的上层对结果进行评估并进行具体操作。

在某些应用中，从安全角度考虑，提前确定 PAN 标识符，以便限制新网络设备只能加入某个特定的网络（必须是已经存在的网络），这种做法是合适的。虽然基于 IEEE 802.15.4 标准的网络可以实现上述功能，但并不推荐这种做法，因为可用的 PAN ID 数量相对有限，而且一旦具有相同 PAN ID 的网络处于相同位置，则从用户的角度来看，可能会有不可预知的情况发生（IEEE 802.15.4 标准中有 PAN ID 冲突的解决方案）。可供选择的替代方法是，所有欲加入网络的设备检测当前网络中的 PAN 协调器的 64 位扩展地址，并将其与自己期望的地址相比较。这样，不管 PAN ID 如何变化，设备仍然能连接到正确的网络。

如果在已有的 PAN 区域创建新的 PAN，此时原有网络或新网络中的 FFD 将成为新 PAN 的专用协调器，新 PAN 协调器要使用不同的 PAN ID，这样所有 PAN 协调器都能够监听到。然而，如果 FFD 的目标仅仅是成为任何网络中的一员，假设 PAN 协调器的状态在信道扫描过程中不变，那么这种情况可能出现多种不同的结果。

如果设备在信道扫描过程中仅接收到一个 PAN ID，那么该设备可能会尝试与

发送该 ID 的设备建立连接。如果有多个设备发送 PAN ID，此时就需要使用选择算法来决定要与哪个设备建立连接。选择算法可能需要考虑接收到的信标帧中一些其他的报文，考虑之前的连接尝试（过去与某个特定设备的连接可能以失败告终），或者采用简单的确定性或随机性过程（例如循环、先入或者随机选择）。

当然，最后一种情况是没有监听到其他 PAN ID。此时，基于应用的考虑，设备不允许成为 PAN 协调器，而将进入休眠状态，休眠周期视具体应用而定，休眠结束后将再次进入信道扫描状态。

6.2.3　信标帧的使用

基于 IEEE 802.15.4 标准的网络将信标帧用作网络发现工具（例如，当前网络希望能吸引新网络设备加入）。信标帧也可用于某个活跃网络的协调和同步（如用作 GTS 控制）。对于希望尽量减少协调器与网络设备间报文传输延迟的某些应用，此时信标帧也将发挥重要作用，因为网络设备可以轻易地检查信标帧中的报文等待区域以确定何时等待报文。

然而，信标帧在某些应用中却是不利的。例如，如果没有报文需要从协调器传输到网络设备，而网络设备到协调器的报文传输量也很少（如无线照明开关），信标帧的传输将消耗协调器的能量，而信标帧的接收又将消耗网络设备的能量。此时，更好的数据传输方式是，当设备有数据要传输时，采用异步传输方式传输其（少量的）数据帧。网络采用星形拓扑结构并且 PAN 协调器使用外部供电时，这种传输方式尤其高效。此时，PAN 协调器将一直处于接收状态下，而网络设备（假设是电池供电的）只有向 PAN 协调器中发送状态变化数据时需要消耗大量的能量。这样，网络设备的电池寿命将大大延长。即使协调器偶尔需要向网络设备发送数据，网络设备也可以让协调器来查询自己的数据，这样设备的电池寿命仍然可以较长。

6.3　星形网络

对于覆盖有限物理区域的应用而言，星形网络拓扑结构是不错的设计方案，此时某个设备（主设备，可作为 PAN 协调器）将处于网络中其他设备（从设备）的覆盖范围之内。基于 IEEE 802.15.4 标准的星形网络使用 FFD 作为 PAN 协调器，而其他设备可以是 FFD 也可以是 RFD。由于星形网络中的设备只与 PAN 协调器通信，与对等网络相比，具有实现上的潜在成本优势，因为在对等网络通信中，设备要存储每个与其通信的节点的报文。符合 IEEE 802.15.4 标准的 RFD，可以作为星形网络中的某个网络设备，这对要求极低功耗的简单点对点应用而言是个不错的选择。

由于星形网络本质上是单跳或双跳网络，报文传输延迟要低于多跳网络。如

果传输延迟是期望应用的一个重要衡量指标，那么超帧中的某个保障时隙（GTS）可能被PAN协调器分配给某个特定的网络设备以预留一定时间，这样能避免信道访问竞争而产生的延时并保证网络设备拥有一定量的带宽。这样，IEEE 802.15.4标准的最大传输延时可低于15.36ms，适合PC外设应用，例如无线鼠标和操纵杆。在极端情况下，可以将单个GTS扩展到信标帧之间的所有时隙。于是，单个网络设备就可以占有整个信道带宽，以满足一些高带宽需求的应用，2.4GHz频段的数据传输速度可以超过115.2kbit/s。

从概念上看，报文在星形网络中的传输不同于在对等网络中的传输。由于星形网络的PAN协调器可以监听所有网络设备，直接控制共享信道的访问，报文在星形网络中的路由可看作发生在MAC层的分组交换，而不是作为网络层中对等设备之间的报文路由算法的一部分。遵循此认识，IEEE 802.15.4标准定义了报文在星形网络中的路由。实际上，MAC层的报文路由在实现时具有一些优势，因为简单的报文转发不需要更高层协议的参与。

6.4 对等网络

IEEE 802.15.4标准的设备也有能力支持对等通信，这样就允许创建多种对等通信网络，每种网络有各自的优势和劣势。下面各小节详细介绍了由IEEE 802.15.4标准中FFD组成的各种对等网络。

6.4.1 扁平网状网络拓扑

最简单的对等自组织网络可能是扁平网状网络，它由一定量的相同网络设备组成，并不是所有的设备都处于任意一个设备的覆盖范围之内。报文从源节点传输到目标节点的过程中，需要大量的路由算法参与。

尽管网状网络中的设备类型可能相同，但是其中某个设备必须具有一些特别的能力来执行PAN协调器的功能，向网络提供其PAN ID，并控制新设备的入网。然而，PAN协调器在报文路由过程中，并不需要承担某个角色。

真正的网状网络通常由一些分散开来的设备组成，这些网络设备可以形成一种通信链路的重复网格模式。然而，此处定义的网状网络允许Ad Hoc设备的布置变得很普遍。

扁平网状网络设计中要解决的主要问题是寻址。由于网络在逻辑上是平等的，网络中没有层次的概念，而且网络设备中没有其他分组或组织形式，所以向设备发送数据时不能根据网络设备的地址来确定合适的路线。然而，针对此类网络，已经设计出了多种路由算法，下面列举出了其中的一部分：

1）洪泛法：发送报文最简单的方式是将每个报文发送给所有的网络设备。尽管这是一个正确的算法（例如，它确实能够将报文传输到目标接收设备），但是这

并不是高效的算法，尤其对基于 IEEE 802. 15. 4 标准的大规模网络而言。向非目标设备发送报文将会消耗大量没有必要的能量。虽然几乎所有的网络都或多或少地需要该算法来传输一些控制和状态报文，但是该算法很少被用于实际网络的数据传输。

2）Bellman – Ford 算法：该算法要求所有网络设备维护一个路由表。该路由表包含该设备到所有其他网络设备的最优路径的路由权值（通常包括一些跳数，也可能包含更为复杂的权值计量，例如路由中设备可用能量状况等），以及路由路径中第一个设备的地址。设备中路由表的维护和更新依靠与其覆盖范围内的其他设备交换报文，然后与目标设备的路由表进行比较选择。报文的路由线路由源设备提前确定，称为源路由。在源路由中，路由报文被作为报文载荷的一部分整体添加到数据单元 MSDU 中；路由路径上的中继设备遵循此路由指令，依次将报文转发出去。Bellman – Ford 算法是解决路由问题的不错方法，但是该算法的动态应对能力并不好。例如，当通信网络中某个连接中断时，该算法自动积聚新路由路径的能量并不强。此外，路由表中的条目要与网络中设备的数量一样多，当网络规模变大后，设备之间彼此交换路由表将变得不切实际。

3）自组织网络梯度路由（Gradient Routing for Ad Hoc networks，GRAd）算法：GRAd 算法要求网络中所有设备都维护一个权值表，该权值表列出了该设备到每个潜在目标设备的路由权值，而 Bellman – Ford 算法维护的路由表中列出的是该设备到网络中所有设备的路由权值。然而，GRAd 算法并不要求网络设备之间交换权值表，报文也不是通过单播方式依据源设备确定的路由路线传输到特定的网络设备的。相反，源设备通过广播的方式，向网络中它能覆盖到的所有设备发送报文，目标设备的路由权值就存储在源设备的权值表中。对于某个设备，如果该设备能够接收到该广播报文，并且其到目标设备的路由权值低于源设备到目标设备的路由权值，那么该设备在等待一段随机时间后转发源设备发出的广播报文，并列出自己的路由权值。

4）蚁群算法：由于蚁群也是自组织、自适应的，所以针对蚁群的生物类推法也已经被探索用于解决路由问题。其中特别有趣的是蚁群的通信方式，蚁群通过在地面上留下信息素踪迹的方式进行相互通信。例如，当外出觅食的蚂蚁发现食物后，将返回巢穴通知其他蚂蚁，同时在地面上留下食物的信息素。其他蚂蚁检测到该信息素，就能到达食物处并返回巢穴，同时留下自己的信息素，这些信息素将汇聚成更宽的踪迹。信息素挥发很快，短时间内没有被使用的信息素踪迹将不会被其他的蚂蚁检测到。这样，蚁群就能快速找出一条通向食物的路径，蚁群中几乎所有的蚂蚁都循着这条路径找到食物。

由于使用信息素的系统为分布式系统，单个蚂蚁的简单个体行为将导致整个大网络的复杂行为，这显然适用于解决路由问题，尤其是当系统中只有一个报文收集源而有多个报文发布源时。可以将报文收集源（例如 PAN 协调器，是所有报

文的目标地址）建模为蚁穴，将发布报文的网络设备建模为食物，网络中中继设备建模为食物和巢穴之间的地面，将报文建模为蚂蚁。PAN协调器周期性发送一个特殊通知报文（包含一个“number - of - hops - taken”的字段），该报文通过单播的方式在网络设备间传输。对于网络中的每个设备，它们都将源设备标识、接收到该报文的邻居设备的标识以及一个时间戳存储到自己的一个数据表中。于是，网络设备增加特殊通知报文中“number - of - hops - taken”字段的值，并转发给一个其他的邻居设备。网络设备将原先存储的报文条目移除，以实现信息素蒸发的功能。

当网络中产生某个真实的报文，且报文的目标设备为PAN协调器，如果源设备最近没有从协调器那里接收到特殊通知报文，这样报文表中就没有关于目标设备的路由条目，则源设备将报文随机发送给某个邻居设备。一直重复该过程，直到报文发送给了具有目标设备路由条目的网络设备。然后，该设备将转发源设备发出的报文给其邻居设备，而这个邻居设备正是给自己发送了特殊通告报文的设备，并且该邻居设备被记录在自己的路由表中。至此，源设备发出的报文就处于“信息素踪迹”上，最终将被转发至目标设备。

蚁群通信模式可应用于某些特定类型的网络，此类网络中只有少量设备作为报文目标接收者，因为每个目标接收者要定期发送通知报文。无线传感器网络就是此类网络的一个典型应用，通常含有多个源设备（传感器）及少量目标设备。

6.4.2　簇形网络拓扑

前面提到的算法，主要针对的是扁平网络，这不可避免地限制了其应用。如果某种网络的逻辑结构在某些方面能有助于路由算法，尤其当网络中的设备数目众多时，那么这种网络结构将更为理想（网络的物理结构仍将是自组织的）。这种网络结构能够避免蚁群算法中大量通知报文的传输，以及Bellman - Ford算法中大量路由权值表的交换。

对许多应用而言，簇形网络拓扑结构是解决该问题的不错选择。在簇形网络中，网络设备节点之间存在父子关系，如图6-5所示。如其他遵循IEEE 802.15.4标准的网络一样，簇形网络在网络形成过程中，PAN协调器是网络中的第一个设备。当有设备连接到PAN协调器上时（设备进而连接到网络中），PAN协调器成为该网络设备的父节点。如果有第二个设备进入第一个网络设备的通信覆盖范围，但是可能处于PAN协调器覆盖范围之外，则第二个网络设备将作为第一个网络设备的子节点而加入到网络中。网络设备可能有多个子节点或孙节点，但是只有一个父节点，如图6-6所示。

新设备通过信标帧来发现网络，包括PAN协调器在内的每个网络设备都定期地广播信标帧。新设备可能会监听到多个信标帧，即新设备有多个邻居设备可作为自己的父节点。此时，新设备最好选择离PAN协调器最近的邻居设备作为自己

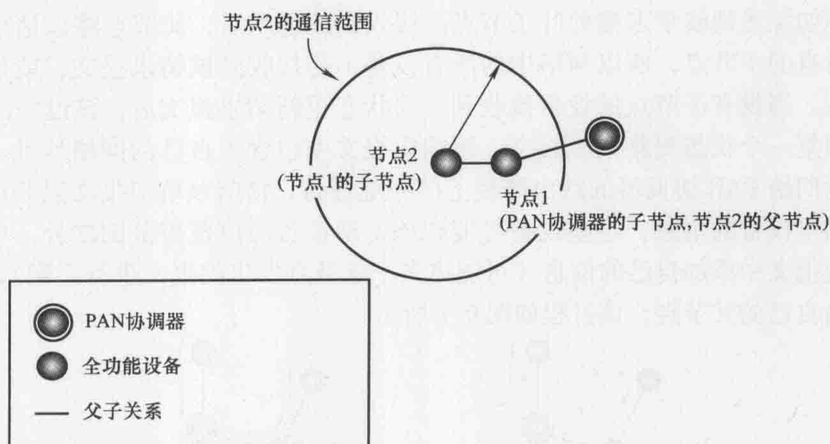


图 6-5　簇形网络形成过程

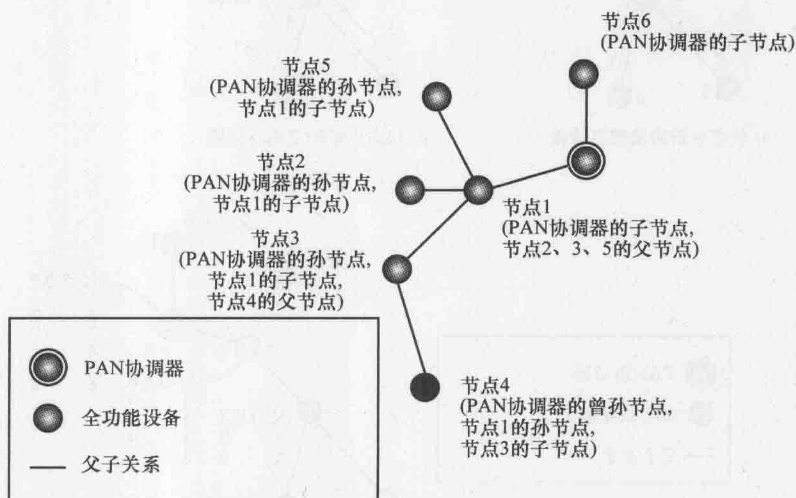


图 6-6　簇形网络中的父、子、孙节点关系

的父节点，一些信息可能被添加到信标帧的载荷中以帮助新设备选择父节点。

簇形网络的结构在一定程度上受 PAN 协调器的控制。不管未来网络将连接何种类型的设备，PAN 协调器在整个网络中一直拥有着权威的作用。PAN 协调器可能会阻止远离 PAN 协调器（到达协调器要经过多次跳转）的潜在网络成员加入网络中，而允许离协调器较近的潜在网络成员加入到网络中，以便形成更为平滑的簇形网络结构，并控制网络中报文传输的时间延迟。

簇形网络的一个优势是它可以方便地实现网络状态周期性的更新，这样，PAN 协调器能够很快发现网络中任何断开的连接和掉线的设备。一种实现状态更新的方法是，PAN 协调器产生状态更新请求报文，并发送至网络中不是父节点的所有

节点，例如发送到枝干末端的叶子节点。接收到该请求后，父节点将该请求转发给自己所有的子节点，所以网络中的所有设备不是接收到该请求报文，就是在转发该报文。当没有子节点的设备接收到一个状态更新请求报文后，该设备向 PAN 协调器回复一个状态更新响应报文，该响应报文中包含了自己的网络地址。在响应报文返回给 PAN 协调器的路由路径上的中继设备，窃听该响应报文以获得该簇中其他网络设备的信息，这些设备可能在该中继设备通信覆盖范围之外。中继设备在响应报文中添加自己的信息（可能将多个子节点发出的报文进行汇聚），然后将转发给自己的父节点，该过程如图 6-7 所示。

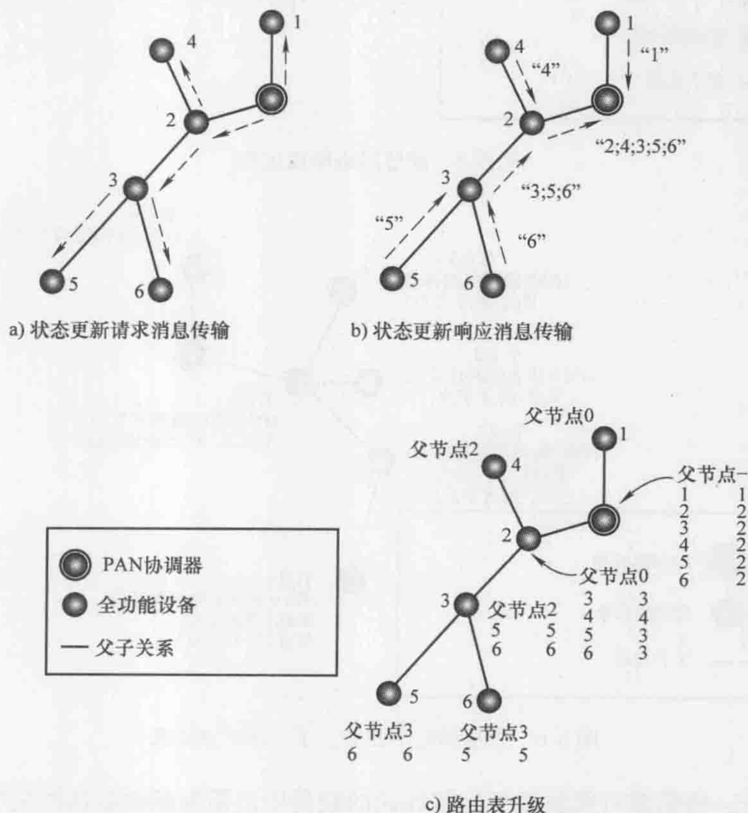


图 6-7 网络中状态更新消息及路由

上述过程的一种变化是，状态更新响应报文中包含每个网络设备的完整路由表。PAN 协调器（事实上，任何可窃听报文的网络设备）可以根据长度增加后的响应报文选择到达相同目标设备的替代路径，这样，当网络设备掉线或者通信连接中断时，这些替代路径可以被使用从而能够提高网络的可靠性。

由于网络设备掌握其周边区域内的网络连接情况，报文在簇形网络中的路由与扁平网络中相比，要更为高效。在簇形网络中一种较为高效的报文路由方式是

使用从状态更新响应报文窃听到的信息。采用这种方法，窃听设备需要维护一个设备列表，该列表列出了该设备的下游设备，状态更新响应报文正是从这些下游设备传输到窃听设备的。这个信息可以被存储在路由表中。

图6-8显示了一种簇形网络中常用的路由算法。假设网络设备都存储着一个由一些条目组成的路由表，该路由表中的条目主要有以下两个来源：

1）通过窃听接收范围内设备而添加的条目。其中的一项条目是关于设备父节点的。这些条目组成相邻设备列表，报文不需要通过中继设备即可被转发到此列表中的所有设备。

2）通过窃听网络状态响应报文添加的条目。这些响应报文可告知设备在其下游网络中所有远离PAN协调器的设备状态。

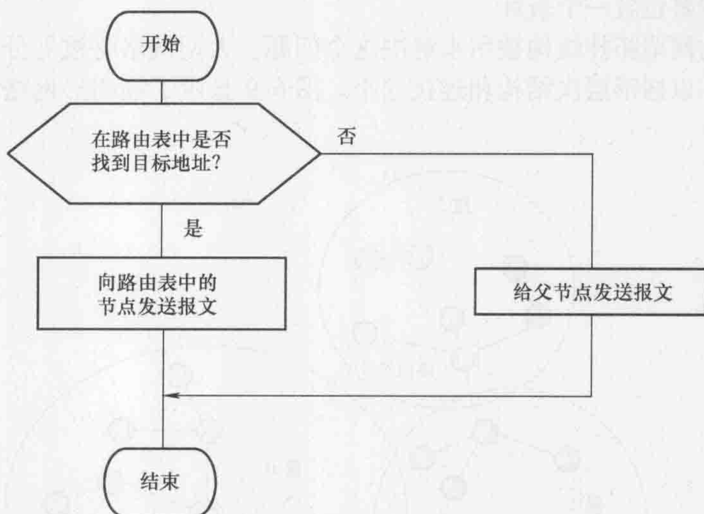


图6-8 簇形网络的一种报文路由算法

按照图6-8中所示的算法，某个网络设备首先检查自己的路由表，查看其中是否有一个条目对应着某个目标设备。如果能找到对应的条目，则报文将被传递给这个合适的设备。如果不能找到对应的条目，报文将被转发给该设备的父节点。由于父节点更加靠近PAN协调器，通过窃听网络中大量设备发出的状态响应报文，父节点拥有更多的路由选择。在特殊情况下，报文也可能一路传递至PAN协调器。

与扁平网络相比，簇形网络结构应用到无线传感器网络中，其一个重要优势在于较小规模的网络设备路由表。通常，对于扁平网络，网络中任何一个潜在目标设备在路由表中都有相应的条目与之对应。而对于簇形网络，其路由表要小得多，因为路由表中没有目标设备，可以通过此设备的父节点来路由报文至该目标设备。路由表的规模减小，对网络设备内存的需求量也随之减小，进而将降低设备的成本。

簇形网络的一个缺点是网络设备间报文传输量的不均匀分布。某些网络设备，尤其是离 PAN 协调器逻辑距离较近的网络设备，相比于离 PAN 协调器逻辑距离较远的网络设备，其报文传输量要高得多，这样将导致网络设备节点间电池寿命的不均匀分布。为缓解此现象，至今已提出了多种解决方法，包括不同网络设备轮流充当协调器，以及到达同一个目标设备使用多条不同的路由路径等。

6.4.3 簇树形网络拓扑结构

IEEE 802.15.4 标准 MAC 层的地址空间，允许网络中存在大量设备节点。然而，随着网络中设备节点的数目不断增加，即使网络采用簇形网络结构，网络设备要维护的路由表规模也将达到不切实际的大小，因为设备的路由表中针对每个子孙节点至少要包含一个条目。

分层次的网络拓扑结构被用来解决这个问题。大型网络将被划分成多个小的簇形网络，并以树形层次结构相连接起来。图 6-9 显示了簇树形网络结构的应用实例。

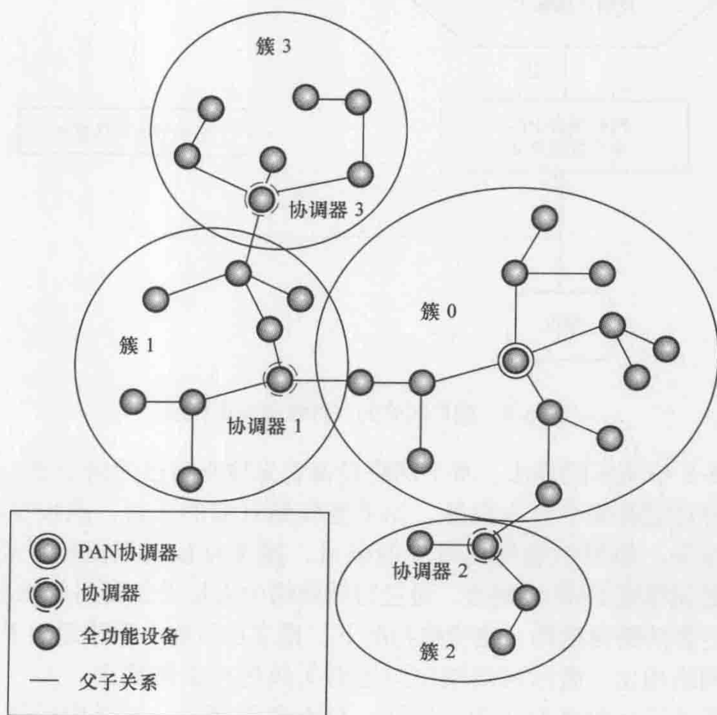


图 6-9　簇树形网络

图 6-9 所示的大型网络由四个小的簇形网络组成，每个簇形网络含有簇首或协调器。簇 0 的协调器，自然而然地成为 PAN 协调器。如果 PAN 协调器有一系列规

则来管理网络的形成，那么簇形网络的形成可能是整个网络形成过程中的一个自然结果。这些规范可能限制了簇形网络中设备节点的数目，或者限制了设备到协调器之间的跳转次数，或者采用了更加复杂的管理算法。如果新网络设备在加入网络的过程中违反了上述规定，PAN 协调器可能还会让该设备加入网络，但是只能作为一个新簇形网络的协调器。

簇树形网络设备的逻辑短地址现在成为具有层次性的地址，由两部分组成：簇形标识符和网络设备标识符。协调器的网络设备标识符和 PAN 协调器的簇形标识符通常置为零。

在簇树形网络中，PAN 协调器仍然能够传输网络状态请求报文。一种实现方式是，像在簇形网络中一样，将网络状态请求报文路由到网络枝干末端，即网络中叶子节点处；网络状态响应报文也以相同的方式处理，只不过报文中的设备标识符被窃听协调器删除了，即离开协调器的网络状态响应报文中仅包含簇形网络标识符。该过程充分利用了设备地址层次化的优势，减小了网络状态响应报文的大小。值得注意的是，在簇形网络中，从每个网络设备路由表中提取出的信息，可能会被添加到网络状态响应报文中以实现路由冗余。

图 6-10 显示了应用于簇树形网络中的可行路由算法。按照该算法，设备首先检查目标设备的簇标识符是否在其路由表中。如果不在，对此设备而言，目标设备为未知设备，设备将报文路由至其父节点。

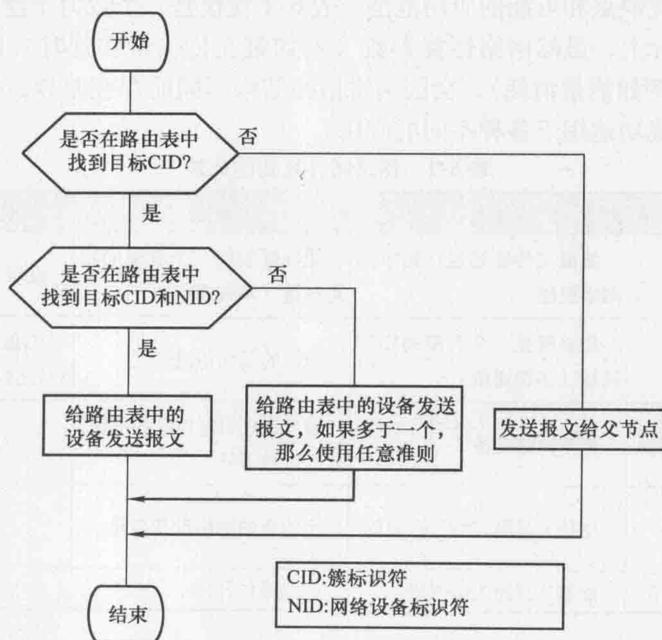


图 6-10 一种簇树路由算法

如果路由表中有相匹配的簇标识符，设备将检查路由表中项目是否与网络标识符匹配。如果找到匹配条目，报文将根据条目进行路由。如果找不到匹配条目，则表明目标设备是已知网络簇中的未知网络设备，设备按照某些仲裁规则来选择适当的网络设备将报文转发出去。

如果目标设备的簇标识符与将要路由该报文的设备的簇标识符相同，报文将如同在簇形网络中一样被路由至该设备的父节点。然而，将报文转发给其他簇形网络的仲裁规则具有更大的灵活性，例如，设备最近转发报文所花费的时间可能会被添加到路由表条目中，因为最新的路由报文能够准确地反映当前网络的情况。其他一些仲裁规则也是可行的，其中许多规则针对某个特殊的应用是最合适的方案。

6.5　网络拓扑决策

由于 IEEE 802.15.4 标准可以支持多种自适应网络拓扑结构，使用该标准的设计师要根据具体的应用需求，选择合适的网络拓扑结构。此外，如果选择的为对等网络拓扑结构，而且其中要使用多跳通信方式，则还要为网络选择适当的路由算法。

作为网络拓扑决策的一个帮助，表 6-1 中列出了本章中提到的主要网络类型，并包括了各自优缺点和可能的应用范围。表 6-1 仅仅是一个致力于建立总体应用趋势的向导。实际上，虽然网络性能参数（例如报文传输量和延时）以及网络设备的性能参数（例如能量消耗），会因网络拓扑结构不同而存在差异，但几乎任何网络结构都可以成功地用于各种不同的应用。

表 6-1　网络拓扑结构的比较

网络类型		优点	缺点	可能的应用领域
星形网络		低报文传输延迟；集中式网络控制	能够覆盖仅一个有限的物理区域（单跳通信）	家居自动化；PC 外设
对等网络		能够覆盖一个大型的物理区域（多跳通信）	较高的报文传输延迟	无线传感器网络；工业监测与控制
	扁平网状网络	简单网络设备	随着潜在目标设备的增加，可扩展性不好	无线传感器网络
	簇形网络	支持大量潜在的目标设备	不均衡的网络设备功耗	HVAC 系统
	簇树形网络	能够支持超大型网络	网络维护开销	工业监测与控制

本部分列出的仅仅是网络结构中的部分实例，还有其他许多没有列出的拓扑结构和路由算法。

第3部分

第7章　系统设计方面的考虑——系统观

IEEE 802.15.4 标准的制定主要针对现有 WLAN 和 WPAN 通信协议在成本、尺寸大小以及/或者功耗等诸多因素无法满足的应用需求。为了能够充分利用 IEEE 802.15.4 标准的能力，达到低成本、小尺寸、低功耗的目的，本章着重描述了在设计系统时需要考虑的一些因素。

为了降低系统成本、尺寸及功耗，IEEE 802.15.4 设备被设计成集成度极高，仅需极少量的外部元件。IEEE 802.15.4 标准中一些特性可帮助实现该目标。

7.1　直接序列扩频

直接序列扩频技术（DSSS）的使用，使得 IEEE 802.15.4 标准的电路实现中大部分是数字电路，仅有相对很小部分的模拟电路。这样的设计使得该标准具有“历史前瞻性”。集成电路光刻技术的提高将增加数字电路的密度，并进一步降低实现电路的功率损耗，这样又能进一步增加 IEEE 802.15.4 标准的优势。DSSS 也具有其他实现上的优势。DSSS 的处理增益能够有效地抑制干扰信号，因此能减少系统对信道滤波器的依赖。借助 DSSS 技术可以简单地设计出正交、多级的信号，这样使得 IEEE 802.15.4 标准 2.4GHz 频段的物理层能够同时具有 250kbit/s 相对较高的数据传输速率（以便迅速完成数据传输并返回睡眠模式）和 62.5ksymbol/s 相对较低的符号传输速率（以最小化在处于活跃状态时的功耗）。上述特性都可以改善系统平均功耗。此外，某些监督管理部门要求扩频通信，DSSS 比跳频扩频（Frequency Hopping Spread Spectrum，FHSS）技术支持更快的网络发现和同步。正是由于这些原因，IEEE 802.15.4 标准选择 DSSS 技术，而非 FHSS 或窄频带技术。

7.2　高信道间隔/调制带宽比

IEEE 802.15.4 标准拥有较高的信道间隔与调制带宽比。这就是说，与信道本身宽度相比，相邻信道远离参考信道。如图 7-1 所示，在 IEEE 802.15.4 标准的

915MHz 频段，第一个空字符的频率与信号中心频率的距离为 600kHz，与相邻信道边缘的距离为 1.4MHz；2.4GHz 频段下，第一个空字符的频率距离信号中心频率为 1.5MHz，与相邻信号边缘的距离为 3.5MHz。这两种情况的信道距离与带宽之比都为 1.4/0.6 = 3.5/1.5 = 2.33。然而，IEEE 802.15.4 标准对相邻信道间隔度的要求很少，只要求与备用信道的有效比例为 3.4/0.6 = 8.5/1.5 = 5.67。相比之下，发送的 IEEE 802.11b/g 频谱，其第一个空字符与信号中心频率间距离为 11MHz，与下一个非重叠相邻信道边界的距离为 14MHz，其信道距离与带宽比率仅为 14/11 = 1.27。IEEE 802.11b/g 标准要求信道有 35dB 的分离度。因此，IEEE 802.15.4 标准信道滤波器带阻远低于正常的滤波通带。高的信道间距/调制带宽比具有以下优越性：

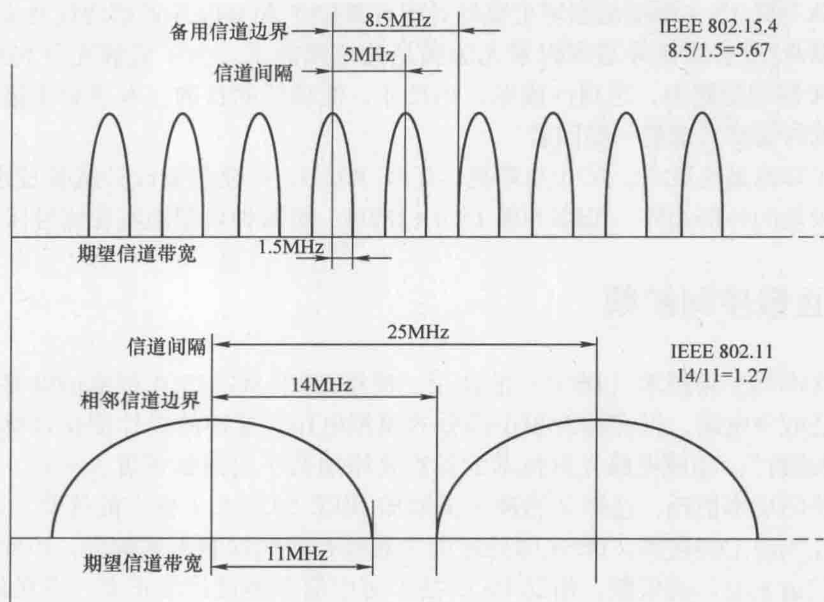


图 7-1　IEEE 802.11 标准与 IEEE 802.15.4 标准中 2.4GHz PHY 选择性需求对比图

1）使用高集成的接收器（例如低中频和零中频架构的接收器）成为可能。不再需要离散表面声波（SAW）、陶瓷或水晶滤波器等器件，能够降低系统实现的尺寸和成本。

2）针对低中频和零中频接收器的实现，信道滤波器的低通截止频率将会升高，从而降低集成的滤波器的大小和成本。

3）需要的信道滤波极点更少，也会降低滤波器的大小和成本。

4）随着更少的滤波极点和更高的转角频率，信道滤波器中达到导通瞬态的时间将缩短，这样接收器启动的时间将更短，进而最小化启动过程中的电池消耗量。

5）相对较大的信道间距意味着信号合成器可能会用到更高的参考频率。由于

合成器的锁定时间与合成器相位侦测器的工作频率相关，所以更高的参考频率能缩短合成器的锁定时间，从而缩短启动时间和延长电池的寿命。

7.3　宽松的传输误差矢量幅度要求

由于 IEEE 802.15.4 标准对接收选择性和发射误差矢量幅度（EVM）给出了相对宽松的要求，这样，接收器振荡器和发射器振荡器的旁带噪声技术规格也可适当放宽，甚至可以放宽至使用低成本的全集成振荡器。该集成振荡器可以是电感－电容（LC）式的，也可以是（更好是）电阻－电容式的，从而可以避免使用尺寸大、成本高的外部压控振荡器以及其他原本也是必需的相关无源元件。

7.4　恒定包络调制

一个减少发射功耗的主要方法是在高频段以半正弦 O－QPSK 方式使用恒定包络调制信号。发射器要设计成适合 IEEE 802.15.4 标准实现的简单电路，电路的直流偏压功率（总发射功耗的一个主要部分）要与峰值包络功率成一定比例。另一方面，在某个给定数据传输率条件下，当确定通信距离的时候（给定某个数据传输率），平均包络功率是一个极为重要的参数。如果选定某种调制方式而且峰值包络功率高于平均包络功率，那么发射器端必然会消耗直流偏压功率和更高的峰值功率。IEEE 802.15.4 标准因此采用了一种恒定包络的调制方式，其峰值包络功率与平均包络功率相等（即峰值与均值的功率比为 1）。IEEE 802.15.4 标准的具体实现可能会利用该调制方案的优势，设计出简单而相对高效的发射器。

7.5　宽松的接收器最大输入水平

IEEE 802.15.4 标准中规定接收器允许的最大输入信号水平为－20dBm，远低于其他 WLAN 或 WPAN 标准的要求。因此，IEEE 802.15.4 标准的系统设计者可以相应地减少接收器前端电流损耗。

7.6　时间和参考频率间的权衡

对于某个遵循 IEEE 802.15.4 标准的具体实现，其时间和频率参考子系统的设计对整个系统的成本和电流损耗有着显著的影响。一个可能的设计方案是在设计时可选用两个参考晶体振荡器，高频振荡器用于 RF 频率参考，低频振荡器是用于协议栈运行的时钟。按照这种设计方案，用于协议栈运行的低频时钟（消耗功率较少）一直处于工作状态，为协议提供时间信息；而用于 RF 频率参考的高频晶振

（消耗功率较高）在发射或接收时刻之前启动，并且在完成相应工作后即关闭，从而使系统的功率消耗降到最低。如果 RF 频率参考要求的启动时间足够短，这样它在整个系统中的能量消耗不占重要地位，那么上述设计方案能够为系统提供较低的平均功率损耗，而只需要为系统添加两个额外的晶振。

另一种设计方案只需要一个高频晶振，同时支持 RF 频率参考和协议栈运行，并一直处于工作状态。高频晶振被分频输出成一个较低的频率，被用作协议栈时钟。当需要 RF 频率参考时，该高频晶振可直接用来作为 RF 频率参考。由于该高频晶振已经处于工作状态，不需要启动时间，因此也不会有额外的能量消耗。由于仅用到一个晶振，所以第二种设计方案的成本要低于第一种设计方案。然而，由于使用了一个高频晶振及分频电路，系统的平均功耗可能更高。系统设计者必须根据应用的具体情况来权衡选择方案。

7.7　单芯片和多芯片实现

集成电路（元件）制造商在进入 IEEE 802.15.4 市场时，要面临这样的抉择：其设计采用两块芯片还是一块芯片。使用两块芯片，则遵循 IEEE 802.15.4 标准的 RF 发射器与协议处理器，分别使用一块芯片（见图 7-2a）。如果使用一块芯片，则 RF 发射器与协议处理器集成到同一片芯片中（见图 7-2b）。单芯片设计具有最高的集成度和最少的集成电路，同时可能有最小尺寸和最低的元器件成本，也可能最适用于没有主处理器的独立应用（下文中将具体讲解）。然而，双芯片设计可能采用更多最佳的集成电路，从而能够更好地满足电路要求（例如 RF 发射器使用 BiC-MOS，而协议处理器使用 CMOS）。与单芯片设计相比，双芯片设计还可以减少产品投放市场的时间。此外，如果支持 IEEE 802.15.4 标准的独立产品具有广阔的市场前景，双芯片设计可以构成多种具有不同协议处理器的集成电路，具有不同数量的内存，并且能经济地支持不同复杂度的多种应用。双芯片设计在选择带一个协议处理器的 RF 收发器时具有一定的灵活性，例如可以选择符合 IEEE 802.15.4 标准的专用发射器或者支持多种标准（例如同时支持 IEEE 802.15.4 和 IEEE 802.11a 标准）的发射器。一个折中的替代解决方案是采用两个芯片，但是将这两个芯片封装在一个芯片里。

7.8　原始设备制造商的具体实现

原始设备制造商在系统设计时面临的问题同样有趣。如果要使某个较大系统具备 IEEE 802.15.4 标准的附加功能，且该系统已有一个通用处理器，那么可使该通用主机处理器运行 IEEE 802.15.4 标准的协议栈，从而不需要额外专门的处理器

来运行 IEEE 802.15.4 标准的协议栈。此时，如图 7-2c 所示，使用更小的一块芯片来仅实现 IEEE 802.15.4 标准 RF 发射器，与上文描述的双芯片设计相比，此种方案能够节约成本。

然而，由于许多协议功能不允许有时间延迟，尤其是当主处理器同时运行着其他实时应用时，软件的集成要复杂得多。例如，需要仔细评估中断处理和任务切换，以确保系统始终有充足的处理能力（如每秒可处理百万条指令和随机存取存储器）。同时，符合 IEEE 802.15.4 标准的发射器和主处理器之间的通信链接，也要考虑到其数据传输能力和消息延迟。当主处理器信息载荷过重时，系统性能将如何恶化通常很难估计或测试，尤其是对于嵌入式系统。如果无法很好地解决软件集成问题，IEEE 802.15.4 单芯片实现方案可被用来分担主处理器的负担，如图 7-2d 所示。

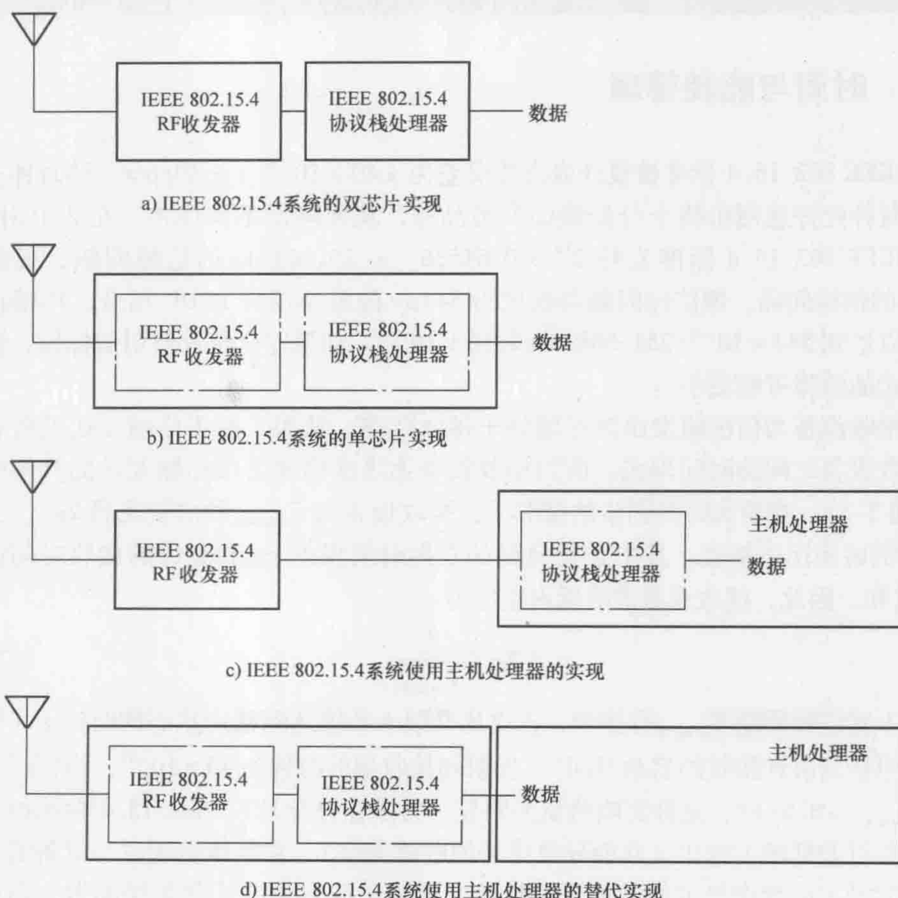


图 7-2　IEEE 802.15.4 标准的多种硬件实现

另一方面，负载轻的主处理器在应对协议栈的实时需求时，面临的困难不大。然而，除非主处理器是针对此类任务设计的，否则当面对 IEEE 802.15.4 协议栈的突发性处理要求时，主处理器不能以高能效的方式处理，而且 IEEE 802.15.4 子系统的平均功耗也可能因此而升高。系统设计者将最能满足预期系统需求的协议组件放置到主处理器上，从而在实现成本与系统功耗之间获得最佳的平衡。

IEEE 802.15.4 标准设计成兼容一些低成本的微处理器，例如基于 8051 或 HC08 内核的处理器，这些微处理器的总线速度仅有几兆赫兹。该设计涉及多个协议层的实用性和灵活性之间的权衡。当协议单独定义为一层时，该设计的软件规模将会有所减小。这种妥协是为了维持这种层次结构，并保持与其他 IEEE 802 协议的兼容，同时尽可能地简化每个协议层。

IEEE 802.15.4 标准最初的设计是使用小封装的微处理器，而现如今，大多数应用都支持射频处理器与 16 位或 32 位处理器相结合。

7.9　时间与能耗管理

IEEE 802.15.4 标准被设计成支持误差为 $\pm 40 \times 10^{-6}$（$\pm$40ppm）的时钟。这样的时钟允许选用价格十分低廉的参考晶振，从而降低系统成本。在 2.4GHz 频段，IEEE 802.15.4 标准支持 $2^{14} \times 0.01536\text{s} = 251.6574\text{s}$ 的信标间隔，或超过 4min 的信标间隔。该信标间隔与长度为 544μs 的最小信标 PPDU 结合，传输占空比可以达到 $544 \times 10^{-6}/251.56824 = 2.16 \times 10^{-6}$。如果完全没有使用信标帧，传输占空比的值将可能更小。

接收设备当信标帧发出时必须处于接收状态。然而，由于信标发送设备和信标接收设备之间的时间误差，所以接收设备无法准确知道信标帧发送的具体时间（见图 7-3）。在没有时间同步的情况下，接收设备每 T_{beacon} 秒内要花费 $2\varepsilon T_{\text{beacon}} + T_{\text{c}}$ 秒的时间用于接收，其中 ε 是允许的发射时间误差 ε_{Tx} 和允许的接收时间误差 ε_{Rx} 之和。因此，接收设备的最低占空比为

$$2\varepsilon + \frac{T_{\text{c}}}{T_{\text{beacon}}} \tag{7-1}$$

不管信标周期 T_{beacon} 有多长，占空比受限于系统达到稳定状态的时钟 ε（该处没有包括发射和接收的启动时间）。发射和接收端的时钟为 40×10^{-6}，当信标帧周期 $T_{\text{beacon}} > 0.5\text{s}$ 时，这种影响将更为明显。为了让符合 IEEE 802.15.4 标准的设备获得尽可能低的占空比（从而导致更长的电池寿命），在具体实现时，设备通常采用的时钟比标准中规定的时钟更加精确。最简单的实现方式为更换晶振，例如将 40×10^{-6}（40ppm）的晶振更换为更加稳定的晶振，但是，这样也会增加系统的实际成本，尤其要求时钟的稳定性限制在 5×10^{-6}（5ppm）以内时。一个更低成本

的解决办法是：认识到同一个设备发出的连续信标帧之间的时间变化是紧密关联的；于是，接收设备可以通过逐条跟踪连续信标帧来减少设备的占空比，因此设备用于接收的时间将小于 $2\varepsilon T_{\text{beacon}}+T_{\text{c}}$ s。

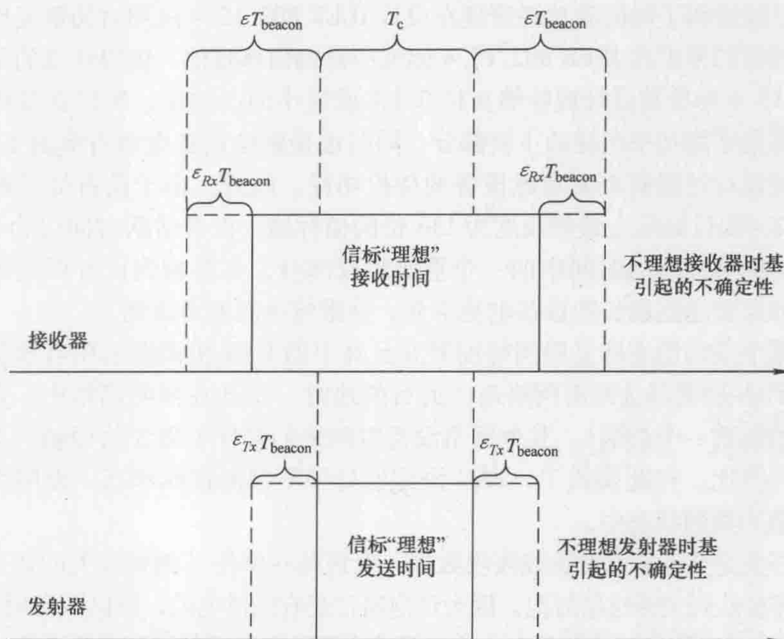


图 7-3　不理想发射器和接收器时间造成的影响

或者，如同其他规范一样，IEEE 802.15.4 标准中可以定义一个时钟偏移规范，可以通过该时钟偏移规范来限制连续信标帧之间可允许的时间差。当 macBeaconOrder = 0 时，显然不需要时钟偏移规范。当 $T_{\text{beacon}}=15.36$ ms 时，与信标 PPDU 长度（在 2.4GHz 频段时为 544μs）和启动时间（至少为 600μs）之和相比，任何可能出现的时钟偏移都显得微不足道。即使设备之间的时钟偏移差异达到 80×10^{-6}（80ppm），与 600μs 比，就算 macBeaconOrder = 7（1.96608s），其偏差值 157μs 也不显著。

当 macBeaconOrder = 14 时，时钟偏移规范也没有用。在长度为 4min 的信标周期内，设备可以由热转冷，改善设备的启动时间只能通过改善时钟的精度，但这种做法通常并不可取。基于 IEEE 802.15.4 标准的单芯片小型应用（使用的可能是纽扣电池）可能具有极小的热惯性。当时钟在一个 16s 的信标周期（macBeacon Order = 10）和极限温度之间时，其变化幅度会比较大，例如可达到 $\pm40\times10^{-6}$（±40ppm）。如果硬件上不添加严格的约束限制（通常成本较高），时钟偏移规范也无法用于此处。在 macBeaconOrder = 10 ~ 14 的范围内时，接收时间必须基于时钟偏移精度规范来规定。

这样，时钟偏移规范的应用范围将限定在 macBeaconOrder = 7 ~ 9 之间。对于低成本的小型协议栈，仅仅为了 3 个 macBeaconOrder 值而规定时钟偏移，显得不切实际。因此，IEEE 802.15.4 协议中并未包含时钟偏移规范。

上文已经说明了时间和功耗管理在设计 IEEE 802.15.4 应用时的重要性，以及针对这些问题的考虑在 IEEE 802.15.4 标准中是如何体现的。值得注意的是，因为 IEEE 802.15.4 标准被设计成能够支持 0.1% 或更小的占空比，所以设备待机时的功率消耗将是平均功率消耗的主要部分，同时也是影响设备电池寿命的主要因素。因此，系统设计过程有必要考虑设备的待机功耗。此外，由于设备的活跃时间有限（对于 2.4GHz 频段上最短长度为 136 位的信标帧，设备活跃时间仅为 544μs），因此启动时间将是活动时间中的一个重要组成部分，将影响到设备可达到的最小占空比。如果要达到最长的设备电池寿命，该影响也需要考虑到。

如果某个应用能支持星形网络配置并且其中的 PAN 协调器采用有线供电，尤其是当该 PAN 协调器为所有网络通信的目的地时（例如在照明网络中，多个无线开关同时控制着一个灯泡），其他网络设备对网络的操作不需要信标帧，即可达到任意低的占空比。在此模式下，PAN 协调器处于不间断接收状态，而网络处于一个持续竞争周期的状态中。

这些开关完全不需要发送或接收数据，直到某些事件（例如开关的切换）引起一个报文需要从开关传送给灯泡。因为灯泡通常是有线供电的，所以该应用可以让灯泡接近 100% 的时间处于接收状态，这样系统中开关的电池使用寿命将格外长。

7.10　天线

基于 IEEE 802.15.4 标准的产品通常要求尺寸较低、成本较低而且功耗较低，因此天线设计的成功与否将直接决定着产品设计是否成功。许多应用场景使用尺寸较小的天线，如果天线部分及其在产品中的安放位置未经过精心设计，那么天线的效率通常不会很高。效率不高的天线，将大大削减发射和接收的范围，这种削减效应造成的影响通常要通过增加发射功率和接收灵敏度来补偿，但这样又会大大减少电池的使用寿命。

通常要在设备物理尺寸、瞬时部分带宽 BW 和电小天线能达到的最大辐射效率 η 之间权衡（例如，具有最大物理尺寸的天线，其辐射效率要远远低于其工作波长 λ）。效率可用下式[24]表示：

$$\eta = \frac{2\left(\frac{2\pi r}{\lambda}\right)^3}{\mathrm{BW}} \tag{7-2}$$

式中，$2r$ 为电小天线的最大尺寸（例如，能够完全包含天线的最小球体尺寸）。

通过上述公式，可以得到以下两个重要的关系：

1）天线的效率与天线的尺寸和工作波长之比的三次方成正比。因此，在更高频段上（更小的波长 λ）的一切操作（包括改变天线的物理尺寸），都会提高天线的效率，这如同增加天线尺寸的同时保持恒定的工作频率。然而，如果天线的尺寸随着波长的变化而变化（例如半波偶极子），则其效率不会受工作频率的影响。

2）设备可达到的部分带宽 BW 与设备的效率 η 成反比。在大多数应用中，即使精心设计的应用于 IEEE 802.15.4 波段的小天线，其效率通常也是比较低的，但足以满足带宽的要求。

天线的附件存在着较强的流动场，例如某些非辐射场。该流动场的强度范围从 d^{-2} 到 d^{-3} 不等，其中 d 是到天线的距离。因此，在距离天线半径至少为 $\lambda/10$ 的区域范围内，流动场的强度非常大。在此范围内的所有介质，包括电池、电路、显示器等，都会对天线的效率产生损耗。设计者应当为产品预留出适当的禁止区域，工作在 2.4G 频段下通常需要预留 1.2cm；而工作在 868MHz 频段下，通常需要预留大约 3.5cm。禁止区域中的介质越多，天线的效率越低。如果产品设计无法满足对禁止区域大小的要求，则实现中应当考虑由此引起的附加效率损耗。如果将较大的天线靠近引起损耗的设备，而将较小的天线远离引起损耗的设备，两者最终的天线效率可能差不多，因为较大的天线导致的效率增加可以与天线附件设备引起的损耗相抵消。

对于小型低成本产品，上述天线设计理论必须要与实际相匹配。由于产品中天线占据的体积不适合给其他元器件（如电路、电池等）使用，所以天线占用的体积通常应被设计成尽可能小。以下因素将影响这类产品的设计：

1）工作频率：正如前文所述，恒定效率下，天线的尺寸随工作波长变化而变化。因此，工作在 2.4GHz 频段下的天线体积较小。

2）工作在多个频段的产品：假设产品可以工作在 868MHz 和 2.4GHz 两个频段，则天线的尺寸要按照较大的 868MHz 频段设计。

3）内部噪声源：由于小型产品中电子元件间的距离较近，即使是相对较弱的噪声源也会对无线发射器产生巨大的影响。典型干扰源包括数字电路（尤其是微型处理器和微型计算机的总线，以及串行数据接口）和开关功率变换器。这些元器件及与之相关的电路板走线应当尽可能远离天线，随着天线尺寸的增大，事情将变得更加困难。如果可能的话，最好能协调控制数字电路的工作，这样，当发射器处于活跃状态时，数字电路处于非活跃状态。

4）外部天线的使用：通常情况，位于产品壳体外部的天线一般效率较高。这些天线通常远离有损耗材料，而且对其尺寸的限制要求更少，因此天线的尺寸可以做得更大。在通信距离较大的应用中如果需要使用定向天线，则外部天线是不错的选择。外部天线也经常出现在无线家用电器（例如电冰箱）中，这类设备的外壳一般是金属结构的。使用外部天线，可以节约更多产品内部空间以供产品中其他元器件使用。然而，与内部天线相比，外部天线的成本要更高，尤其当外部天线要与 RF 连接器配合使用时。由于外部天线缺少产品外壳的保护，将更容易受

环境、操作及其他因素的影响而出现机械故障。天线与发射器之间馈线上的损耗也是产品设计时要考虑的一个因素。

如果确定使用内部天线，产品设计时将会有多种选择。其中一种选择是电路板天线，由于不需要购买、处理或布置天线在电路板上，所以电路板天线肯定是成本最低的一种方案。然而，这种实现方案也不是完全免费的，因为电路板本身需要购买。虽然成本低廉，但是这种方案也有其不利因素，电路板天线往往损耗严重，这可能是由于电路板天线的磁阻（由较细的铜线引起）和与损耗材料的距离较近而引起的。损耗材料有多种，例如电路板本身材料、附近地线、电路板上的布线以及其他各种电路元件。

导线天线，如圈型天线和偶极子天线，可以被放置在电路板上方以增加其效率。导线天线综合了外部天线的高性能和电路板天线的低成本。由于天线的机械结构和尺寸等都会对其谐振频率产生影响，为达到最好的性能，在使用之前通常要对天线进行调谐。在某些具体应用中，还需要为其提供非金属材质的支架。

陶瓷材料的专用天线，其物理尺寸要比导线天线更小，而且不需要调谐。但是，其价格也比导线天线更高。

7.11　产品设计的灵活性

IEEE 802.15.4 标准被设计成能灵活地应用于各种各样的应用，从个人计算机外设和玩具到家居自动化再到工业控制领域等。这些应用对成本、尺寸、电耗等的要求各不相同，因此针对某个应用的理想设计不一定适用于其他应用。图 7-4 是一个蜘蛛图，显示了空间、成本和电耗因素对三种不同应用的相对重要性。上述影响因素仅仅是个别实例，会因实现细节和特定的应用不同而表现出很大的差异性。

如图 7-4 所示，成本是家居自动化应用中最为重要的考虑因素，而电耗的重要程度最低，因为家居网络可以有线供电。类似地，电耗因素在工业控制应用中最为重要，而尺寸因素的重要程度最低，因为此应用的对象可能是某个大型工业发动机控制器。最后，尺寸因素是 PC 外设应用（例如无线鼠标和游戏杆）中最重要的因素，而成本因素的重要性最低。应用设计者应当根据具体应用要求，在上述三种因素之间权衡来最优化某个 IEEE 802.15.4 产品。

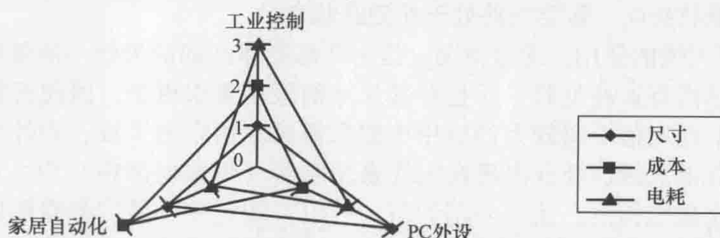


图 7-4　性能参数相对不同应用的重要性的案例

第 8 章　现实世界中的问题——接触现实

IEEE 802.15.4 标准的用户、开发者及系统集成者应当意识到，一旦涉及“现实世界”，诸多方面的因素将会影响到系统的性能。IEEE 802.15.4 标准的产品与其他射频产品的共存，不同通信协议间的对接，就是其中的两个重要因素。

8.1　共存

IEEE 802.15.4 标准物理层使用的两个频段几乎在所有国家都是免授权的，所以多种不同协议的设备通常共享该频段。例如，868MHz 频段上存在有专有的低数据传输速率协议；915MHz 频段上存在有专有协议和无绳电话设备；2.4GHz 频段上有无绳电话、微波炉设备，以及无线局域网和无线个域网等网络。在大部分国家，工作在免授权频段的设备被要求能够接受工作在该频段上其他设备的干扰，并且该设备的用户无权对其他系统引起的设备性能下降提出合法的赔偿。虽然规章如此，但是市场并不这样认为；购置新设备的用户有理由要求新设备不但能正常运行，而且不会干扰已有设备的操作。所以，不能满足这两个准则的设备很难在市场上立足。因此，共存就成为一个重要的经济问题。

IEEE 802.15.4 标准的许多特性，就是为了能够与其他系统共存而设计的。尽管共存问题可以分为两个方面：①保护其他系统免受 IEEE 802.15.4 系统的干扰；②保护 IEEE 802.15.4 系统免受其他系统的干扰。但是实际上，大多数针对某一方面的解决方案也适用于该问题的另一方面。下文列出了 IEEE 802.15.4 标准中的一些特性，这些特性能减少对其他系统的潜在干扰，其中的许多内容源自 IEEE 802.15.4 标准中的“共存附录”。

1）低发射功率。尽管世界上许多地区（包括 FCC 规范[25]中的 15.247 部分）的无线发射法规允许 915MHz 和 2.4GHz 频段具有相对较高的发射功率（某些情况下约为 1W），但是符合 IEEE 802.15.4 标准的设备可以工作在远低于此发射功率的条件下。IEEE 802.15.4 标准的一个关键指标是低成本，并且要求低成本的片上系统射频芯片可以实现超过 10dBm 的发射功率。尽管这个要求技术上可以实现，但从经济层面上看却是不利的。此外，FCC、欧洲规范组织（ETSI EN 300 220 - 1 V1.31[6]）、CEPT 倡议 70 - 03[5] 和 ETSI SN 300 - 328[7] 中关于电磁辐射的规定，使得设备的发射功率在不增加额外且昂贵的滤波器的前提下超过 10dBm 变得困难。这些因素将超过 10dBm 发射功率的设备限制在某些特定的应用。

2）信道划分。许多基于 IEEE 802.15.4 标准 2.4GHz 物理层的系统，都需要

考虑与基于流行的 IEEE 802.11 标准的 WLAN 之间的共存问题，尤其是最多采用 3 个不重叠 WLAN 信道的 WLAN 设备。图 8-1 显示了北美不重叠 IEEE 802.11b/g 信道与 IEEE 802.15.4 标准信道的划分。在北美地区，不重叠 IEEE 802.11b/g 信道编号分别是 $n=15$、20、25、26；在欧洲地区，不重叠 IEEE 802.11b/g 信道编号分别是 $n=15$、16、21、22。这 4 个符合 IEEE 802.15.4 标准的信道位于 3 个 IEEE 802.11b/g 频段之间（或之上）的防护频段。尽管 WLAN 信号在这些防护频段上的能量值不为零，但是却低于该信道中其他信号的能量。因此，IEEE 802.15.4 网络运行于这些防护频段上能够最小化 IEEE 802.15.4 系统与 WLAN 系统之间的干扰。动态信道选择（由上层控制）可在网络初始化或对受损信道做出响应时执行。此时，符合 IEEE 802.15.4 标准的设备将扫描一系列由 MLME－SCAN.request 原语中信道列表参数指定的信道。对于安装在 IEEE 802.11b/g 系统活跃区域内的 IEEE 802.15.4 标准网络，信道列表参数可被定义为一些集合（集合［16，23，28，29］、［16，18，24，25］或其他合适的集合），以满足最大化 IEEE 802.15.4 网络与 IEEE 802.11b/g 网络的共存。

3）信道选择。在网络形成之前，候选的 PAN 协调器扫描信道列表中的所有信道，以识别出已有的 IEEE 802.15.4 网络。如果找到适合的 IEEE 802.15.4 网络，候选的 PAN 协调器在网络层的控制下可能会选择加入该网络，而不是创建另一个网络。这种方式能够尽量减少同一频段中不同 PAN 的数量，因此也就减少了对其他系统的潜在干扰。如果没有找到合适的 IEEE 802.15.4 网络，候选的 PAN 协调器将创建新的 PAN，并从信道列表参数（由能量检测信道扫描确定）中选择未被占用的信道来供新的 PAN 使用。第二种方式能够避免在已被某些系统占用的频段上传输数据。

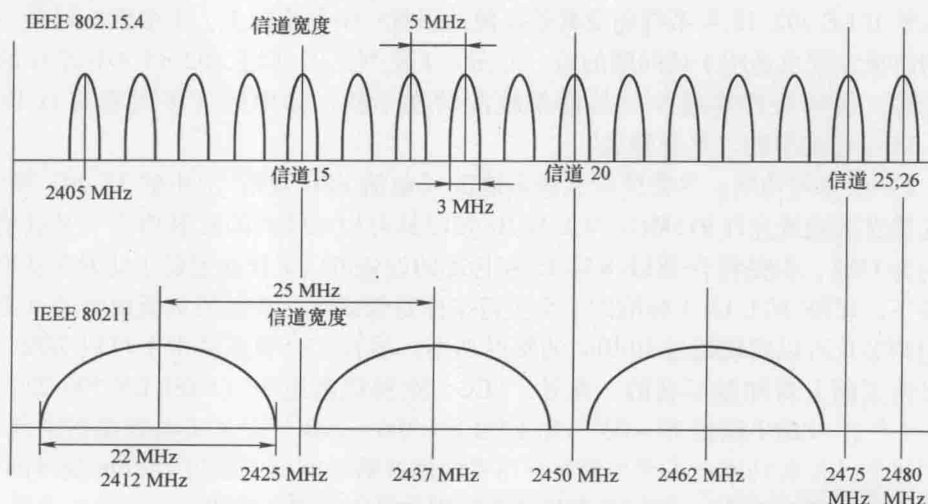


图 8-1　北美不重叠 IEEE 802.11b/g 信道与 IEEE 802.15.4 标准 2.4GHz 物理层信道的划分

如果在PAN占用的信道上出现干扰现象，PAN协调器协议栈中的上层将执行动态信道选择算法（未在IEEE 802.15.4标准中定义）。首先，PAN协调器扫描其信道列表中的可用信道，并为PAN选择新的信道。然后，该PAN协调器返回原来被干扰的信道，向整个PAN发送广播报文，以告知PAN转移到的最新信道。该过程有助于避免IEEE 802.15.4系统与其他系统之间的相互干扰。

1）空闲信道评估。IEEE 802.15.4标准中的CSMA-CA信道评估机制，可以在数据传输之前执行一次空闲信道评估（CCA）。IEEE 802.15.4的物理层要求至少使用以下三种CCA方法中的一种：①超限能量检测（ED）；②IEEE 802.15.4信号的检测；③上述两种方式的结合。当某个设备欲使用某个信道来发送数据时，如果该信道已被其他设备占用，不管这些设备使用的是哪种通信协议，该设备的传输服务都将暂时避退，这种方式即是超限能量检测（ED），它能改善IEEE 802.15.4系统与其他系统之间的共存。

2）扩频技术的使用。IEEE 802.15.4标准中使用的直接序列扩频技术，可以为使用窄频带（例如频段小于200kHz）通信协议的用户提供某些保护，即将250kbit/s的数据传输扩展到频带宽度大于2MHz的频段上，这样能够减少IEEE 802.15.4设备在任意窄带信道上的发射功率以保护自己提供的服务。有趣的是，尽管IEEE 802.15.4信号被扩展了，由于其低数据传输速率，IEEE 802.15.4标准的传输带宽与IEEE 802.15.1标准（蓝牙）的传输带宽仍具有可比性。其结果是，IEEE 802.15.4的PAN与蓝牙PAN之间的相互干扰作用与两个蓝牙PAN之间的相互干扰作用相似——只会影响到蓝牙79个信道序列中的3个信道。

3）链路质量指示。IEEE 802.15.4标准的物理层定义了链路质量指示（LQI）。LQI可由每个接收到的分组反映出来，可以通过接收到信号的强度、信噪比估计，或者两者的综合来反映。LQI可用于检测由于数据报冲突而引起的信道干扰，为上层应用提供有关信道状况的实时信息，方便设备有根据地做出动态信道选择。

WirelessHART标准巧妙地融合了IEEE 802.15.4标准提供的各种共存机制，以应对工业环境对无线射频的挑战，从而提供了高可靠性的通信。本书的第4部分将详细地说明工业级别的共存是如何实现的。

8.2 同一位置上收发器的安装

有些系统带有两个射频（RF）收发器，例如有些手机同时支持手机网络和WPAN网络。这类系统的设计者应当意识到，两个射频收发器之间可能会彼此相互干扰。许多具体应用中要求这种设计，即手机设备作为PAN协调器，同时还作为WPAN和Internet之间的网关。此时，干扰可能是由辐射及传导效应引起的。

将两个RF收发器置于同一产品中时（或者实际上距离很近），首先要考虑其中一个设备的发射噪声辐射对另一个设备接收器的影响。所有收发器在传输实际

信号之外，也传输了一定量的宽频带噪声，噪声频率范围通常在信号附近几百兆赫内。因为噪声的振幅通常很小，不会对信号造成严重后果，因此从经济角度考虑，不需要增加滤波器或者其他电路来进一步降低噪声。然而，如果接收器（更确切地说是接收天线）非常靠近传输天线，此时噪声将变得很大。这种情况下，即使两个收发器工作的频段差距很大，其中一个设备发送时引起的噪声也将会明显地影响第二个设备的接收灵敏度。如果两个收发器使用的通信协议相互独立，一个收发器接收数据的同时，另一个收发器也可以传输数据。一些其他的手段，例如控制收发器的输出，也可使两收发器能同时正常工作。

第二个辐射效应为接收器阻塞效应。阻塞，作为一种很强的信号效应（与噪声效应相反），发生于高强度且是非期望的信号进入接收器并影响其电路的偏压直流时。这种干扰通常会引起增益衰减，进而导致灵敏度的下降。在一定程度上，阻塞效应影响了接收器检测到的信噪比中信号的比例，而宽频段传输的噪声影响了其中噪声的比例。例如，发射功率为600mW的蜂窝收发器与低功耗WPAN接收器置于相同位置时，阻塞现象将会发生。如果入侵信号（offending signal）的频率在受干扰接收器的传输频带之外，阻塞效应的改善可以通过在接收器输入之前添加滤波器，或者也可以在接收器的电路中增加偏压直流（即增加能量消耗），但是通常不建议使用第二种方式。

两个收发器公用同一电源将会引起传导效应。对于便携式设备，这种现象常常是不可避免的，因为其主要能量供给来源于电池，而不管从尺寸还是重量角度考虑，都不可能为设备配备第二块电池。然而，当一个收发器分掉公用电源中大量电流时（通常发生在收发器发射时），任何内部或者外部电阻引起的公用电源的电压下降都将影响到另一个收发器的正常工作。这种现象的一个教科书式例子是由一个基于时分多址（TDMA）的蜂窝式收发器引起的电源电压调制，例如一个GSM（全球移动系统）收发器，由于其以音频速度传输信号，从而导致在早期GSM手机里有可听得到的谐音。这个问题可以通过适当的电源设计来纠正，但是通常需要为受损害设备附加独立的电压调节器。

第4部分

第9章 WirelessHART的介绍——在过程控制应用中使用IEEE 802.15.4

WirelessHART（或IEC 62591）是一种基于IEEE 802.15.4标准的工业无线网络。WirelessHART的拟定用途是针对工业过程自动化的监测和控制应用，其中工业过程自动化包括制药、石油和天然气、纸浆和造纸、水/废水处理、化工以及其他工业工厂应用。对于无线通信，这些应用比住宅和商业应用要求更高的可靠性和安全性。此外，工业应用要求无线网络能覆盖很广的区域，且能容纳大量的无线设备。

对于大多数的网络系统而言，少量的通信分组丢失是正常的。然而，对于工业网络系统，这种分组的丢失是不可接受的。对于工业应用，特别是连续流程工业应用，无线传感设备要求能够无中断地运行好几年。正如在后文中所要介绍的，这个重要的可靠性要求已经通过在WirelessHART设计中添加多个系统冗余而得到解决。

安全性在工业网络中也是一个非常严厉的要求，重点在于过程数据的保密和过程数据的完整性。例如，在简单的水箱水位监测中，各供应商在因竞争原因进行商业谈判时，应保持水位信息的保密性。同样的，一个装有有毒化学物品的容器的水位信息应该是正确的（没有被篡改）。否则会存在一定的风险，即有毒液体的溢出将会危害工作人员和周围的环境。由于无线通信系统不能像有线通信系统那样被物理保护起来，所以针对工业应用的无线通信系统应该强制性地要求信息安全技术。

在工业控制应用程序的设计者和操作员心中的安全有以下几个要求：

1）防止非法或非期望的网络渗透。

2）防止在适当的和预期的操作中有意或无意的干扰。

3）防止不适当地访问机密信息。

WirelessHART并没有制定一个很复杂的系统来满足重要的可靠性和安全性需求。简单是WirelessHART的一个基本特色，从而在增加系统鲁棒性的同时允许非熟练工人的全部操作。

利用 IEEE 802.15.4 标准，WirelessHART 也解决了工业车间操作员使用标准化技术的需要。标准能让用户采用多个厂商的同类设备、促进相互间的竞争、降低产品的价格和提高产品的质量。

此外，对于来自不同厂商的不同类型的设备，如果它们遵循相同的通信标准，那么它们彼此间就可能产生相互作用和进行交互操作。这种多厂商的方法保证了市场上会有多种类型的设备。最后，维护良好的标准会随着时间的推移变得更加稳定，并且通常能保持与先前版本的向后兼容性，避免使用专用技术带来的一些问题。

一个工业生产车间通常需要上千个设备作为生产自动化的基础。因为所有传感器的测量数据都应该被实时传输，即数据必须在一个预定的时间内被发送和接收，所以大量设备间的协调将成为一个挑战。该预定的时间即为通信允许的延迟。典型的工业过程自动化传感器设备的延迟范围 1 ~ 100s。

通常，工业过程自动化生产车间的覆盖区域比较大，WirelessHART 通过提供网状网络技术，来允许大区域范围内的设备间的相互通信。设备可以为其他设备转发数据。

WirelessHART 技术使用 IEEE 802.15.4 标准定义的 2.4 GHz ISM 频段。由于工业应用遍布全球，所以它需要一个全世界范围内都可用的无线频段。正如本书前面章节所介绍的，使用 2.4 GHz ISM 频段带来了一个额外的好处，即不需要授权。然而，WirelessHART 技术不得不与其他技术（如 ZigBee 和 802.11/Wi - Fi）共享该频段。802.11/Wi - Fi 与 WirelessHART 有着特别的关联，因为遵循 IEEE 802.11 标准的系统在很多工业应用中被广泛作为骨干网络。WirelessHART 选择 IEEE 802.15.4 标准是因为该标准提供了与 IEEE 802.11 标准的高度共存。

WirelessHART 标准是在 2007 年 9 月 12 日发布的。2010 年 3 月，WirelessHART 被 IEC 采纳作为一个国际标准，同时在 2010 年 7 月被欧盟采纳作为 EN IEC 62591。

9.1　可寻址远程传感器高速通道

可寻址远程传感器高速通道（HART）协议是一个全球标准，它用于在设备之间的模拟线路上发送和接收数字信息，并控制或监控工业系统。HART 是用于工业过程自动化领域的主要通信系统。HART 协议在 20 世纪 80 年代后期得到发展，并在 20 世纪 90 年代早期发展为 HART 通信基金会。

HART 实际上是过程测量仪表的工业标准，并有超过 20 年的历史。超过 2600 万个已安装的 HART 设备，超过了全球工业仪表总量的 50%。HART 标准随着时间不断发展，并一直保持着向后兼容，每次 HART 标准的改变都是向标准中添加功能且不删除任何东西；当前版本（HART 7）第一次引入了无线技术。WirelessHART 是 HART 7 标准的一部分。

HART 协议定义了开放系统互联（OSI）7 层协议模型的第 1、2、3、4 和 7 层。HART 是一个双向通信协议，该协议提供了智能现场仪表和上位机系统之间的数据访问。上位机可以是技术员的手持设备或笔记本电脑中的任何软件应用程序，也可以是工厂过程控制、资产管理、安全系统或其他控制平台中的任何软件应用程序。

HART 通信协议在其最高的协议层提供了三种应用命令：

1）通用命令：这些命令适用于所有的传感和控制设备，包括诊断和设备标签。

2）常规命令：这些命令适用于大部分的传感器和执行器，主要侧重于校准和动态范围调整。

3）设备特定命令：这些命令代表了每个现场设备具有的独特功能。设备供应商定义这些命令。

一些 HART 协议中定义的通用和常规命令见表 9-1。

表 9-1　HART 通用和常规命令的例子

通用命令
读取制造商和设备类型
读取主要变量和单位
读取电流输出和量程百分比
读取最多四个预定义的动态变量
读取或写入 8 个字符的标签，16 个字符的描述符、日期
读取或写入 32 个字符的报文
读取设备量程值、单位和阻尼时间常数
读取或写入最终装配代码
写入轮询地址
常规命令
写入阻尼时间常数
写入设备量程范围值
校准（调零，设置范围）
设置固定输出电流
执行自测试
执行主复位
消除主要变量的零点
写入主要变量的单位
消除 DAC 的零点和增益
写入传递函数（平方根/线性）
写入传感器序列号
读取或写入动态变量赋值

9.1.1　WirelessHART 技术

HART 通信基金会决定在 HART 传统技术的基础上发展一个无线技术，以提供

一些额外的能力。这些能力使得 HART 能够被用于工厂的某些区域，而有线 HART 系统应用到这些区域可能并不经济或在技术上难以实现。同时，WirelessHART 兼容传统的 HART 技术和产品，从而允许已布置在现场的这些设备可以完全地加入到 WirelessHART 网络中。WirelessHART 设备使用与有线 HART 设备相同的命令结构，并且使用相同的软件平台和相关的工具。

在普通的无线网络上传送 HART 协议报文无法满足工业无线应用的要求。工业无线应用要求一定程度的实时控制、可靠性和安全性，而这只能通过定义一个基于 HART 扩展而来的体系结构并最小化协议开销。

除了 ISO 7 层模型，WirelessHART 也规定了将设备集成到一个工业控制系统的方法。其中一个例子就是设置传感器的操作范围、标签、警报、输入类型等。

通过使用 HART 基础设施，一个集成的 WirelessHART 解决方案提供了一个低成本的解决方案。使用标准的 HART 命令，用户可以使用现有的配置设备来配置和维护现场仪表。

此外，基于 WirelessHART 的无线系统提供了安全传输，以避免数据的窃取和改变。WirelessHART 确保了其安全性能满足过程工业的最严厉的要求。

9.1.2　电池寿命

为了增加电池的使用寿命，WirelessHART 规定了一种智能报告，即 WirelessHART 设备只有当被要求时或某个过程变量发生变化时才发送数据。此外，WirelessHART 系统使用时分复用来调度设备在网络中的通信，这样可以让设备大部分时间处于睡眠状态。例如，WirelessHART 系统可以对电池供电的设备进行通信调度，使其可以在不更换电池的情况下工作很多年。最后，调度好的时隙可以被用来发送异常数据报告（例如警报和事件）。WirelessHART 的时分复用也为过程变量（PV）的信息传输提供了一个时间戳，从而可以增强通信的实时性。

9.1.3　集中式网络协调

WirelessHART 中的时分复用机制和其他一些功能都是集中式的。时间协调确保了 WirelessHART 网络可以正常运行，并可避免网络设备间由于时间偏差而引起的冲突，同时还可以最小化与其他系统的干扰。

使用集中式协调功能，网络管理器可以对影响网络性能的因素实时地做出响应，并重新调度网络通信以避免拥挤的网状路由，以及由于堵塞、多径衰落或干扰而引起频段可用性的下降。

集合了所有这些性能的 WirelessHART 标准简化了设备的安装过程，同时提供了一个开放的网络，从而使得来自不同制造商的设备能够在 WirelessHART 网络内互操作。

9.2 WirelessHART系统

WirelessHART使用IEEE 802.15.4标准定义的2.4GHz工业、科学和医疗（ISM）无线电频段。WirelessHART使用了直接序列扩频（DSSS）技术和跳信道技术，来保证通信的安全性和可靠性，以及在网络设备之间提供基于TDMA的同步通信和延迟控制的通信。通过大量过程工业现场的试验和应用，这种技术已经被证明具有非常高的可靠性。

WirelessHART网状网络中的每个设备都可以作为路由器来为其他设备转发报文。换句话说，设备可以不必直接与网关进行通信，而只需要将报文转发给下一个最近的设备。这种做法延伸了网络的覆盖范围，并可以通过提供冗余路由路径来增加通信的可靠性。

WirelessHART网络管理器根据延迟、吞吐量、效率、能耗和可靠性来确定冗余路由路径。为了确保冗余路由路径的可用和畅通，报文应该交替地在多跳冗余路由路径上传递。因此，就像互联网一样，如果某个报文通过一条路径不能到达它的目的端，那么它将被自动重新路由到另一条好的冗余路由路径，且不会有数据丢失。

WirelessHART的网状网络结构也使得添加或移除设备变得简单。只要一个设备在其他网络设备的范围内，该设备就可以进行通信。

为了满足不同应用需求所需要的灵活性，WirelessHART支持多种报文模式，其中包括：

1）过程量和控制量的单向发布。

2）自发异常情况通知。

3）自组织的请求/响应。

4）大块数据的自动分割和传输。

这些功能允许对通信进行调整以适应不同的应用需求，从而降低功率损耗和开销。

一个额外的功能与仪表调试有关。WirelessHART系统被设计成可以使用现有的基于HART系统的调试工具，使得新仪表设备加入网络的过程变得简单和安全。

9.2.1 WirelessHART的共存

WirelessHART系统被设计成可以最大限度地共存于2.4GHz频段。这是通过以下多种共存措施来实现的：

1）建立在IEEE 802.15.4标准定义的空闲信道评估和信道黑名单基础上的信

道质量评估。

2）跳信道机制以避免繁忙的信道和尽量减少多径衰落的影响。

3）基于 TDMA 的时间多样性。

4）使用持续时间较短的数据分组（好邻居）。

5）可变的发射功率。

6）网状网络提供的路径多样性。

WirelessHART 使用跳信道技术在多个频率间不断切换以传输数据。这种做法能防止潜在的、具有破坏性的无线电信号阻塞 WirelessHART 数据的传输。WirelessHART 使用了 IEEE 802.15.4 标准提供的直接序列扩频技术，由于该技术具有能量扩展和代码分集，所以 WirelessHART 系统能最小化对相同频段内其他系统的影响。

WirelessHART 定义的媒体访问控制（MAC）帧头也被用于进一步确保与其他基于 IEEE 802.15.4 标准的网络（如 ZigBee）的共存。这种方法的关键是帧头键值的区别：如果一个 ZigBee 设备接收到一个来自 WirelessHART 设备的报文，ZigBee 设备将丢弃该报文，反之亦然。

时隙允许周期性地传输数据，还允许报告异常数据（如警报、警告、事件）。WirelessHART 网络中的每个设备都是时间同步的，因此每个数据分组都包含有一个时间戳。无线网络中的所有设备共享某些可用的 ISM 频段。为了实现一个有效的通信协议，每个网络设备都需要进行时间同步，以避免彼此间的通信冲突以及同步数据的发送和接收。WirelessHART 系统将时间分成很多个时隙，并将这些时隙分发给每个网络设备，这样网络设备就能及时地访问网络。

每个 WirelessHART 设备都会被分配一定量的时隙以适应所需的数据发布率，这样每个网络都可以支持仪表以不同的速率发布报告。设备在安装过程中需要设定设备的数据发布率。时隙的分配是自动的，且基于每个设备的数据发布率。

由于时间同步，每个设备都知道跳信道所使用的信道序列，这确保了 WirelessHART 传输设备和接收设备不仅在时间上是同步的，在频率上也要是同步的。

9.2.2 WirelessHART 网络的可靠性

上述共存机制不仅允许其在 2.4GHz 频段的和睦操作，还将 WirelessHART 系统的可靠性提升到了一个很高的水平。例如，负荷试验显示：20 多个设备组成的 WirelessHART 网络能拥有 99.999% 的数据可靠性。有了此可靠性性能，我们可能会观察到系统会有无线分组的丢失。然而，由于多冗余机制，WirelessHART 系统可以无差错运行。

WirelessHART 协议包含以下三个关键的组成部分，它们有助于提高端对端通

信的可靠性、简化安装过程和提高电源效率：

1）基于时间同步的通信：充分利用了通信容量和能量存储。

2）跳信道：减少了干扰的影响，同时减小被窃听的风险。

3）完全冗余的网状路由：提供了一个健壮且可根据外部环境的变化而动态调整的网络。

符合 WirelessHART 标准的设备将可以与其他供应商的 WirelessHART 设备实现互操作，并支持有线 HART 和 WirelessHART 的工具。

时分多址访问被用于调度网络上的通信。一个 WirelessHART 的调度被定义为一系列 10ms 的时隙，以便协调数据的传输。这样的设置可以减少能量消耗，消除网络中的通信冲突，以及同步传输以有效利用带宽和减少通信延迟。此外，TDMA 机制允许使用冗余的时间调度。

WirelessHART 是一种集中控制式的网状网络。该网络中的每个设备都可以传输自己的数据，同时还可以转发来自于其他设备的信息。这种关键特性提供了高可靠的端对端数据通信。每个现场设备都拥有两条或更多的路由路径来发送数据至网关。当某条预定的路由路径因干扰被暂时堵塞时，这些冗余路由路径将被用作替代路径。如果一条路由路径被永久堵塞，那么新的路由路径将会自动建立。

WirelessHART 网状网络允许每个设备都有冗余路由路径至上位机系统。WirelessHART 网络管理器自动分配这些路径以维护实时冗余控制。

9.2.3 网络设备类型

图 9-1 显示了 WirelessHART 定义的网络设备。工厂自动化网络可以是一个标准的网络，或者是一个专有网络。WirelessHART 网关可以通过 WirelessHART 接入点连接到 WirelessHART 网络。多个 WirelessHART 接入点可以增加网络的吞吐量和提高无线网络的整体可靠性。

以下几种类型的设备可以连接到 WirelessHART 网络：

1）现场设备。

2）适配器。

3）路由器。

4）网关。

5）手持设备。

所有 WirelessHART 网络设备都能发送和接收 PPDU，并可以执行网络形成和维护所必需的一些基本功能。所有网络设备都发起和收集分组，还可以转发其他网络设备发出的分组。每个网络设备还拥有一些属性，以存储与更新率、会话和设备资源相关的信息。其中，会话和设备资源包含一些条目，例如超帧的长度。

此外，所有的网络设备在出厂时都被分配一个唯一的标识号（ID）。这个唯一的 ID 遵循 IEEE 扩展唯一标识符（EUI）一样的格式。IEEE EUI 由两个部分组成：

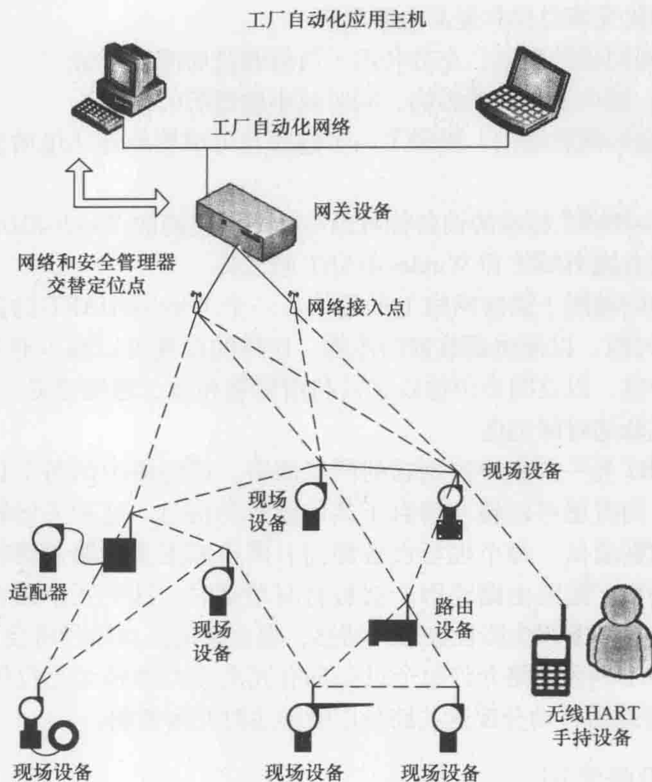


图 9-1　WirelessHART 网络的组成

第一个部分是一个由 IEEE 登记机关分配给 HART 通信基金会的 24 位的组织唯一标识符（OUI），第二个部分是一个 40 位的扩展标识符。

1. 现场设备

现场设备被直接连接到工业过程以实现测量和/或控制。它是数据分组的生产者和消费者，也能够路由其他 WirelessHART 网络设备发出的数据分组。现场设备可能是有线供电、回路供电、电池供电或以其他某种方式供电。

WirelessHART 网络中的每个设备都可以路由数据分组。然而，网络管理器根据网格优化算法和用户提供的约束条件来控制每个设备的路由能力。

2. 适配器

适配器设备为非本地的通信设备提供到无线网络的物理连接和逻辑连接。适配器使非本地设备看起来像一个 WirelessHART 现场设备。它使用内部路由表来协调无线网络和非本地通信子设备之间的通信流量。WirelessHART 适配器不是直接连接到工业过程的，但它支持所有现场设备需要的命令，包括代表非本地连接的现场设备来发布过程数据。在响应 WirelessHART 网关发出的识别命令时，它将报文中设备标志字段设置为 0x04（即协议转换桥设备）。

WirelessHART 允许实现一种特殊类型的 HART 适配器。这种适配器通过有线的方式（4~20mA）与现有的 HART 仪表相连，同时作为一个网络设备加入到 WirelessHART 网络，从而可以将该 HART 仪表的数据通过 WirelessHART 网络传递到上位机应用程序。这种适配器可以位于沿 4~20mA 仪表电缆的任何地方，它可能是电池供电或从该 4~20mA 电缆获得电能。

3. 路由器

路由器是一种特殊的设备，它被设计成只为一个网络设备转发分组到另一个网络设备。它通过网络资源来找到下一跳邻居设备，即接收到的分组将要被转发到的地方。

在 WirelessHART 中，因为所有网络设备都具备路由能力，所以单独的路由器是不需要的。然而，添加额外的路由器对于提高网络中的路由可能是有益的，例如可以延伸网络或节省现场网络设备的功耗。路由器通常不与工业过程监测仪表直接相连。

4. 网关

WirelessHART 网关设备连接 WirelessHART 网络到一个工厂自动化网络，并允许在两个网络之间传递数据。它使得上位机应用程序可以访问 WirelessHART 网络设备。网关设备可以被用于将一种协议转换到另一种协议，或将命令和数据从一种格式转换为另一种格式。WirelessHART 网络也可以使用 WirelessHART 网关来作为时间同步的时钟源。WirelessHART 规定每个 WirelessHART 网络拥有一个逻辑网关。

虽然一个 WirelessHART 网络只存在一个逻辑网关实体，但也有可能设计多个网关以实现与多个网络的连接。

网关功能在逻辑上包括一个网络接入点（或仅仅是接入点）、一个网络管理器和一个安全管理器。然而，这些组件中的每一个都可以在物理上被一起绑定在一个网关设备里，或者物理地分布在不同的网络硬件中。

WirelessHART 网关为无线网络通信提供了一个汇聚点或源点。网关还提供了到网络管理器的连接。网络中的网关通过一个固定的唯一 ID（0xF981000002）来识别。此外，网关位于所有网络图（Graph）的根部，这样就允许协议数据单元（PDU）被路由到最方便的网络接入点。接入点担任网络层路由器的角色，其拥有一个唯一的设备 ID 和网络地址。

网关使用应用层服务来与网络设备进行通信。此外，网关还可以担任服务器的角色，负责收集和维护来自网络中所有设备的缓存的数据和命令响应。这些缓存的命令响应包括发布数据报文、事件通知和命令响应。缓存的命令响应被立即返回给上位机应用请求程序；这将有利于减少网络通信载荷，并提高能量的利用

率和上位机应用程序的响应性。

5. 网络接入点

网络接入点，也称作接入点，通过提供到无线网络的接口来允许 WirelessHART 网络和网关之间的互联。网关可以使用多个网络接入点来提高网络的有效吞吐量和网络的可靠性。

网络管理器负责配置接入点中的路由。当一个 WirelessHART 网关使用多个网络接入点时，网络管理器可以为每个网络设备提供冗余路由。

网关和它的任何一个逻辑组件（如接入点、网络管理器和安全管理器）之间的通信是在 WirelessHART 标准范围之外的。

网络接入点传播时钟到现场网络；总是至少有一个网络接入点执行此任务。如果有不止一个网络接入点，那么网关要确保它们各自的时钟要彼此保持同步，这将导致以下三种情况：

1）一个网络接入点（见图 9-2）。

2）多个网络接入点，每一个网络接入点都提供网络时钟（见图 9-3）。

3）多个网络接入点，其中至少有一个网络接入点不提供网络时钟（见图 9-4）。

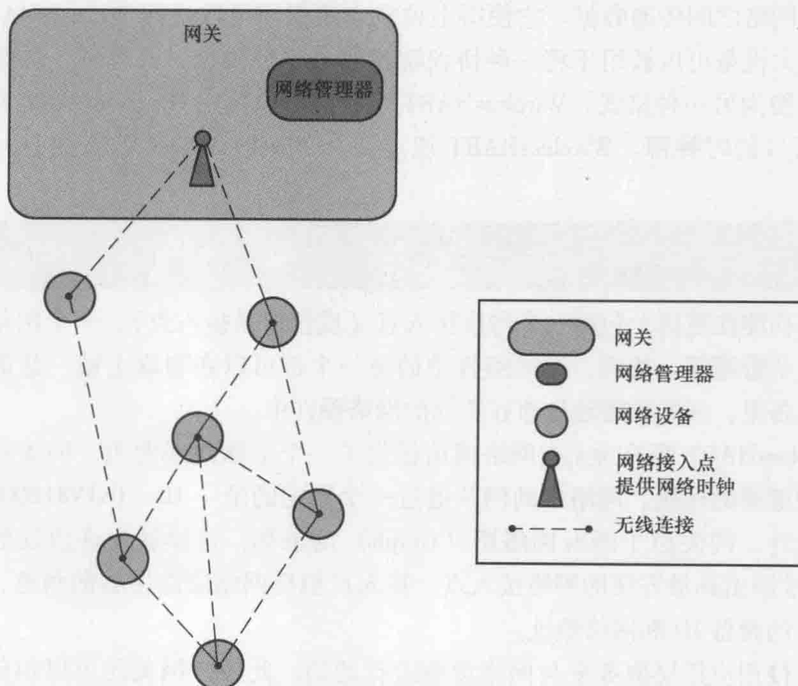


图 9-2 带时钟的单个网络接入点

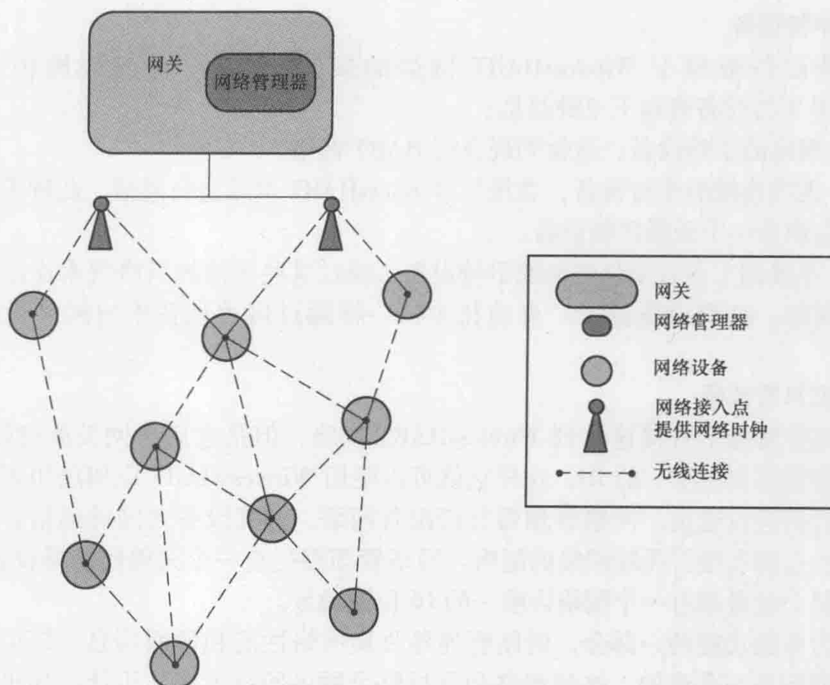


图 9-3　提供网络时钟的多个网络接入点

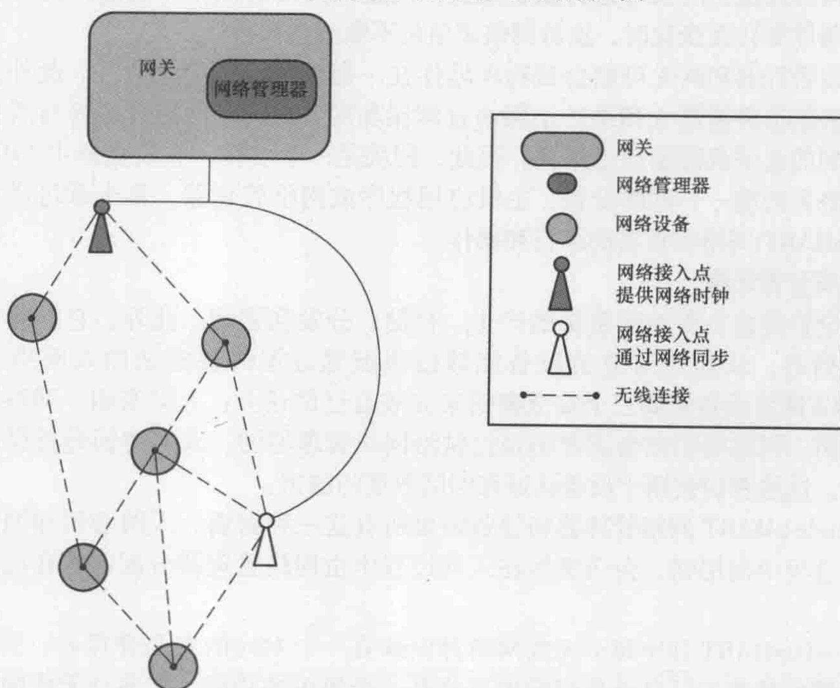


图 9-4　不提供网络时钟的多个网络接入点

6. 手持设备

手持设备被用于 WirelessHART 网络的安装、控制、监测和维护。WirelessHART 手持设备有以下三种类型：

1）有线的手持设备：连接到现有的 HART 网络。

2）无线连接的手持设备：直接与 WirelessHART 网络进行通信。此种手持设备入网后会作为一个无线现场设备。

3）连接到工业自动化网络的手持设备：通过某些其他的网络技术连接到工厂自动化网络。这种设备像工厂自动化主机一样通过网关设备来与网络设备进行通信。

7. 网络管理器

网络管理器不直接连接到 WirelessHART 网络，但是它属于网关的逻辑部分。网络管理器有自己唯一的 ID，这样它就可以使用 WirelessHART 应用层协议来与其他网络设备进行通信。网络管理器负责配置网络、调度设备之间的通信、管理路由表以及监测和报告无线网络的健康。网络管理器拥有一个完整的网络设备列表，并保证每个设备都有一个网络内唯一的 16 位短地址。

作为系统功能的一部分，网络管理器收集网络性能和诊断信息。该信息在系统运行期间是可获得的，这使观察和分析整个网络的行为成为可能。如果检测到问题，网络在运行时就可进行重新配置。当整个网络的操作和性能因为环境载荷和环境条件变化而变化时，这种网络调整将不断地被执行。

网络管理器和网关可能会被物理地连在一起或者也可能会分开。此外，一个安全通信信道将被建立和维护于网络管理器和网关之间。网络管理器与所有网络设备之间的通信都需要通过网关；因此，网关是一个实体，它负责路由 PDU 到指定的网络目的端——网络设备、主机应用程序或网络管理器。第十章将详细介绍 WirelessHART 网络管理器的运行和操作。

8. 安全管理器

安全管理器负责加密密钥的产生、存储、分发和管理。此外，它拥有被授权设备的列表，从而让对应的设备能够按照配置政策的规定来加入网络。WirelessHART 网络设备需要三个安全密钥来完成自己的任务：入网密钥、网络密钥和会话密钥。网络密钥和会话密钥是提供给网络管理器的，入网密钥是提供给网络设备的。这些密钥被用于设备认证和网络数据的加密。

WirelessHART 网络管理器和设备需要所有这三种密钥。入网密钥和网络密钥在入网过程中被用到。会话密钥在入网过程中由网络管理器分配，并在此之后被使用。

WirelessHART 规定每个无线网络都应该有一个对应的安全管理器。然而，安全管理器在某些工厂自动化网络中可能是一个集中的功能，为多个无线网络提供服务，并且在某些情况下也可能为其他网络和应用程序提供服务。

WirelessHART 标准没有定义安全管理器的功能需求和运行，也没有定义它与网络管理器的通信。第 12 章将展开介绍 WirelessHART 安全和安全管理器相关的话题。

9.2.4　电源和电源管理

WirelessHART 设备的供电方式可以是有线电源供电、电池供电、能量收集设备（如太阳能、振动）供电或它们的一个组合。

正如后文中所介绍的，一个网络管理器集中协调一个 WirelessHART 网络。网络管理器负责为每个网络设备定义一个基于时分复用的超帧结构，并动态分配时隙给每个网络设备。时隙调度的目的是维持特定工业仪表的通信需求。为了省电，网络设备在没有通信调度的时候可以变得不活跃（即进入睡眠状态）。

此外，作为 WirelessHART 系统电源管理机制的一部分，WirelessHART 设备周期性地报告自己的电源状态；这样如果它们是电池供电，那么它们的电池在用尽之前就可以被提前更换掉。

9.2.5　电子设备描述语言

传感器和执行器的管理是一个不间断的过程，它以最初的安装为起始，然后进行周期性的校准，在设备整个生命周期内诊断设备，以确保设备和工厂车间可靠运行并拥有高性能。为了避免安装和维护过程中的错误，集成到控制系统（或被用于设备管理的独立系统）中的软件通常提供一个用户界面，这个用户界面按照一种统一的方式显示了设备制造商所期望的设备信息。

电子设备描述语言（EDDL）是一种基于文本的、特定领域的语言，它通常被用在工业应用中来描述现场设备的特点。EDDL 技术使用标准化的工具来管理整个产品的生命周期，从而可以集成工业产品信息。

此外，如图 9-5 中的例子所示，EDDL 非常灵活，它可以用来描述拥有多种不同通信接口（如 HART、WirelessHART 和 PROFIBUS）的设备，或拥有更高层解释器的设备。

EDDL 为主机系统和手持设备访问和显示现场仪表中的信息提供了一个标准化的形式和结构，它独立于通信协议或设备操作系统。EDDL 提供了一种特定领域的语言以描述工业自动化系统组件的属性，这些组件包括通用的数字和模拟输入/输出模块、运动控制器、人机界面、传感器、闭环控制器、编码器、液压阀和可编程序控制器等。由 EDDL 描述的属性包括：

1）设备参数和它们的从属关系。

2）设备功能，例如仿真模式和校准。

3）图形显示，例如功能表。

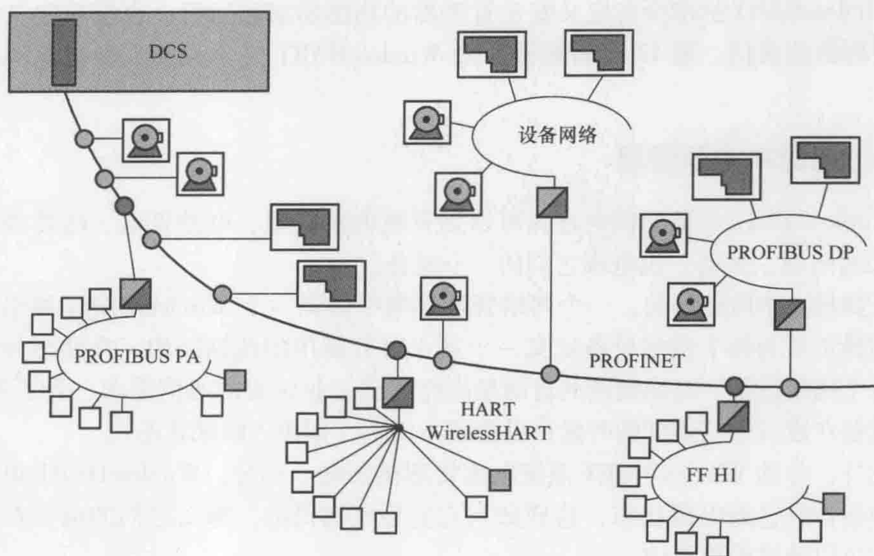


图 9-5　通过 EDDL 集成不同现场总线网络设备的示例

4）控制设备之间的相互作用。

5）图形显示。

① 增强的用户界面。

② 图形系统。

6）永久数据存储。

IEC 61804-3 标准以一种与语法无关的方式定义了 EDDL 的语义和词汇结构。从 ISO/OSI 模型的角度来看，EDDL 位于第七层之上。然而，EDDL 应用程序使用通信系统来传输它的信息；EDDL 包含了一些结构用来支持映射到某个通信系统，当然这里的通信系统包括 WirelessHART。

EDDL 还描述了将要显示给用户的信息的管理。然而，这种可视化的具体表示并不是 EDDL 标准的一部分。

9.2.6　映射 WirelessHART 到 ISO/OSI 基本参考模型

ISO/IEC 7498-1 模型的原则、方法和模型被用来设计 WirelessHART 协议。ISO/OSI 模型提供了一个通信标准的分层方法，其中各层可以被独立地开发和修改。WirelessHART 标准定义的功能覆盖了 ISO/OSI 协议栈从顶部到底部的各层，其中很多包括协议栈用户所需的功能。图 9-6 所示的是简化的现场总线模型，ISO/OSI 的中间 3~6 层的功能可以按照此模型进行合并。此时，WirelessHART 的第 5 和 7 层被融合到现场总线的应用层，第 3 和 4 层被融合到现场总线的数据链路层。

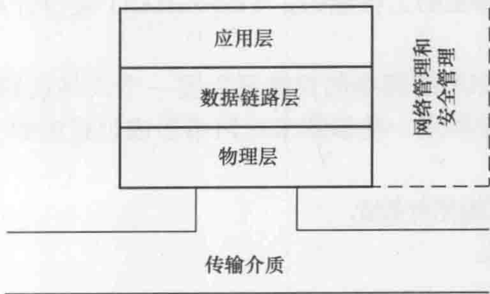


图 9-6　基本现场总线参考模型

表 9-2 显示了 ISO/OSI 参考模型的各层以及各层的功能，还显示了 WirelessHART 参考模型中的等效层。

表 9-2　ISO/OSI 和 WirelessHART 协议层

ISO 层	功能	WirelessHART 层
7 应用层	将协议栈中的命令转换成底层能够理解的格式，反之亦然	面向命令的、预先定义的数据类型和应用流程 ↑ ↓
6 表示层	将数据转换成标准的网络格式	
5 会话层	创建和管理下层的会话	
4 传输层	提供透明的、可靠的数据传输（可能涉及多个链路的跨网络的端对端传送）	大块数据的自动分割传送，可靠的数据流传输，可协商的分块大小 ↓或↑ 功耗优化，冗余路径，自愈合无线网状网络 ↓或↑ 安全 & 可靠，时间同步 TDMA/CSMA，带 ARQ 的频率捷变
3 网络层	执行报文路由	
2 数据链路层	通信介质的接入控制和错误检测（一条链路上的点对点通信）	
1 物理层	将数据编码和解码成以适合于通信介质的发送/接收的信号；规定通信介质特征	2.4GHz 的无线频段，基于 IEEE 802.15.4 的无线射频技术，10dBm 的发射功率

注意：↓和↑表示当前层的功能可能按照箭头指定的方向被包含在现场总线的协议层中。这样，网络层和传输层的功能可能被包含在数据链路层或应用层，会话层和表示层的功能可能被包含应用层而不被包含在数据链路层

9.2.7　WirelessHART 网络规划和安装

通常，任何一个无线网络的安装都需要仔细地规划，以确保其性能和可靠性能达到一定的要求，这对于有线网络和无线网络都适用。通过由网络管理器所提

供的自我配置和自我修复的工程能力，WirelessHART 被设计成尽可能地简化规划和安装过程。

用于形成 WirelessHART 网络的设备只需要一个入网密钥和网络密钥。然而，管理器允许操作员通过利用一些参数来对网络形成过程施加一些约束，这些参数包括：

1）针对特殊应用的拓扑控制。

2）网络大小控制。

3）传播延迟控制。

4）网络设备更新率。

5）冗余路径的配置规则。

6）信道黑名单。

7）路由功能的运用。

8）多个接入点之间多播选项的处理。

网络管理器中的优化算法不是 WirelessHART 标准的一部分。不同的实现要么可以提供一个简单的配置界面，这可以隐藏网络内部的复杂性；要么可以提供一个更复杂的控制界面，这将暴露网络内部的一些部件。

第 10 章　WirelessHART 网络

正如前面章节所强调的，WirelessHART 网关提供 WirelessHART 现场设备与主机网络（如 PROFIBUS）之间的连接。虽然网络管理器和安全管理器的功能都可以存在于主机应用层里，但是网络管理器和安全管理器可以驻存于 WirelessHART 网关中。

WirelessHART 网络的形成过程由 WirelessHART 网络管理器发起。WirelessHART 网络管理器包含建立和维护 WirelessHART 网络的必要算法。同时，WirelessHART 网络管理器还实时分析来自于 WirelessHART PDU 的服务信息质量，以鉴定最佳路线、调度（10ms 时隙的分布）、频道和其他参数，从而保持在一个预定的性能水平。

WirelessHART 标准并没有规定如何实现安全管理器、网络管理器和网络接入点。在早期 WirelessHART 实现系统中，网络管理器、安全管理器和网络接入点都建立于网关硬件平台上。然而，这样的体系结构是供应商自定义的。WirelessHART 下一代产品正在将网络接入点、网关和网络管理器分离开来。

WirelessHART 网络中的每个现场设备都有路由报文的能力。然而，网络管理器控制着网络设备的实际路由功能。对于特殊的应用程序，网络管理器可根据任何具体准则，禁用某个现场设备的路由功能。然而，手动的方式不建议被用来禁用路由功能，因为它可能会使网络管理功能欠佳。例如，它可能会降低某些网络设备的功耗，但是可能会增加其他网络设备的功耗，或者产生其他副作用（如增加了 WirelessHART 网络中的拥堵点）。运行有优化程序的网络管理器，在其服务质量参数中已经考虑了电池寿命的最大化和通信管理的最优化。

10.1　网络自愈

WirelessHART 网络允许使用专用路由设备或路由器。这些设备没有被连接到工业过程，但有助于扩大 WirelessHART 网络的覆盖范围。此外，这些专用的路由器还有助于提高 WirelessHART 网络的鲁棒性，例如，避开现有的或新的障碍物。

每个 WirelessHART 网络设备在网络管理器的命令下路由报文，此内置功能简化了网络的规划和部署。此外，这种功能是 WirelessHART 无线网状网络具备自愈能力的一个关键元素。

10.2　网络维护

网络管理器负责调度时隙、管理动态信道分配和确定路由路径（包括最优和

冗余路径），以保持一个指定的服务质量水平。网络维护活动包括发现潜在的邻居设备，收集与邻居设备之间的通信信道有关的统计信息，以及维护每个网络设备的时间同步。为了增加可靠性，WirelessHART 网络中的每个网络设备都维护有一个可与自己直接通信的邻居设备列表。为了处理 RF 环境的动态变化（如传播效应和多径衰落等），网络设备保持其当前的邻居设备列表。

Advertise DLPDU 和 Keep - alive DLPDU，这两种特殊的数据链路 PDU（DLPDU）用来建立和维护邻居设备列表。这两种 DLPDU 中包含有足够的信息来使新邻居被发现，或者让新安装的设备请求加入网络。如果该请求被接收，那么该新设备就可以成为公告设备的一个邻居设备。作为自己网络管理算法的一部分，网络管理器可以调度这些 DLPDU 的传输。

每次与邻居设备的成功通信都确认了邻居设备的存在，并允许评估它们之间通信链路的链路质量。因为通信仅发生于当设备需要向其邻居设备发送一个 DLPDU 时，所以链路不被使用的时间间隔可能会比较长。此时，Keep - alive DLPDU 可被用来探测静态链路和维持设备间的时间同步。

10.3　WirelessHART 网络拓扑结构

WirelessHART 网络可以被配置成不同的拓扑结构以支持各种不同的应用需求，例如：

1）星形网络：星形网络（见图 10-1）只有一个路由器设备，该路由器设备与几个终端设备通信。路由器设备也可以是网关的网络接入点。这是 WirelessHART 网络中最简单的网络拓扑结构。一个星形网络适合于小规模的、覆盖低的应用。本书中的第 3、5 和 6 章涉及了一些星形网络相关的话题。

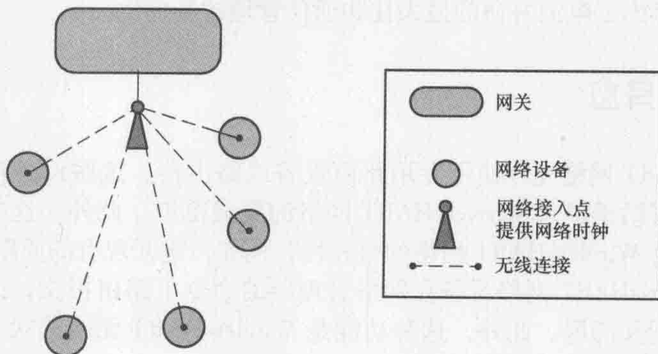


图 10-1　WirelessHART 星形网络的拓扑结构

2）网状网络：网状网络（见图 10-2）由一些网络设备形成，这些网络设备全部是路由器设备。网状网络提供了一个健壮的网络，它有冗余的路由路径来适应 RF 环境的变化。本书中的第 5 和 6 章涉及了网状网络的一些细节问题。

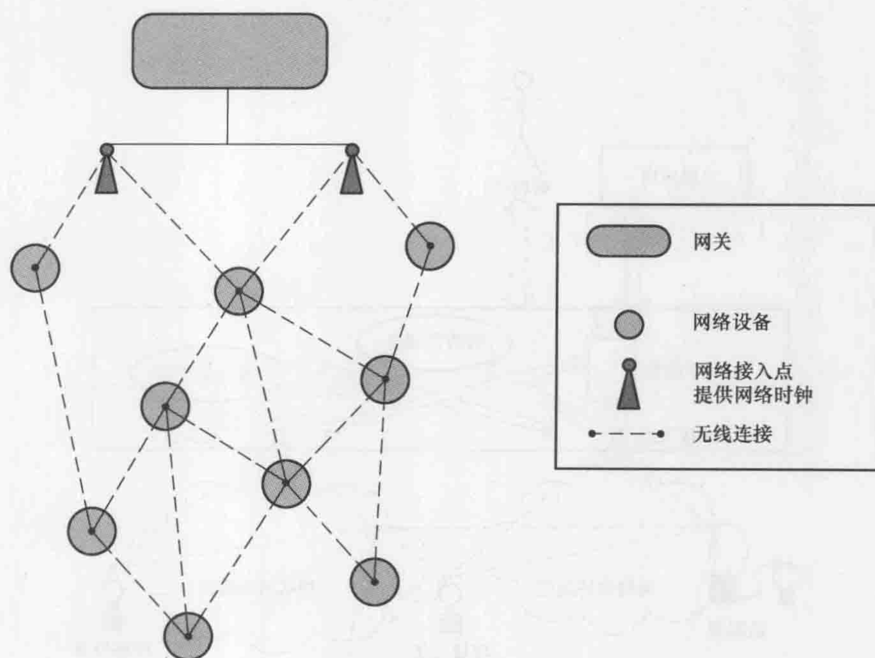


图 10-2　WirelessHART 网状网络的拓扑结构

3）星形 - 网状网络：星形 - 网状网络（见图 10-3）是星形网络和网状网络的结合。在本质上，此拓扑结构只是另一种类型的网状网络。

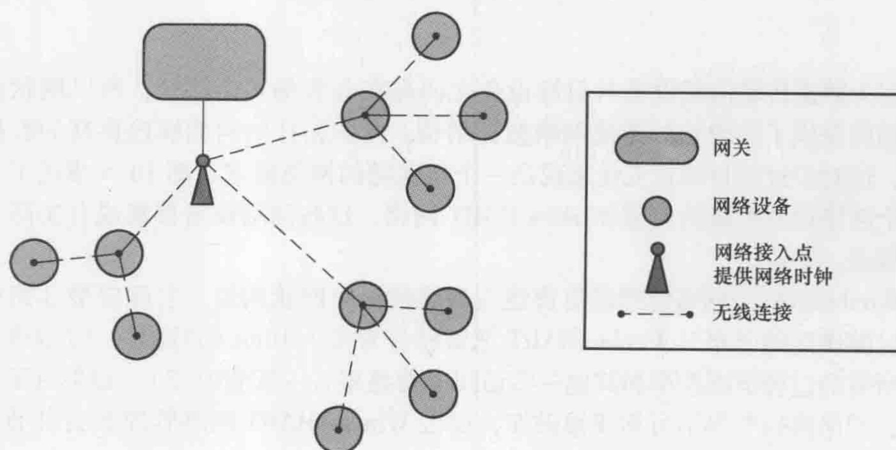


图 10-3　WirelessHART 星形 - 网状网络的拓扑结构

图 10-4 显示了一个可能的冗余结构。

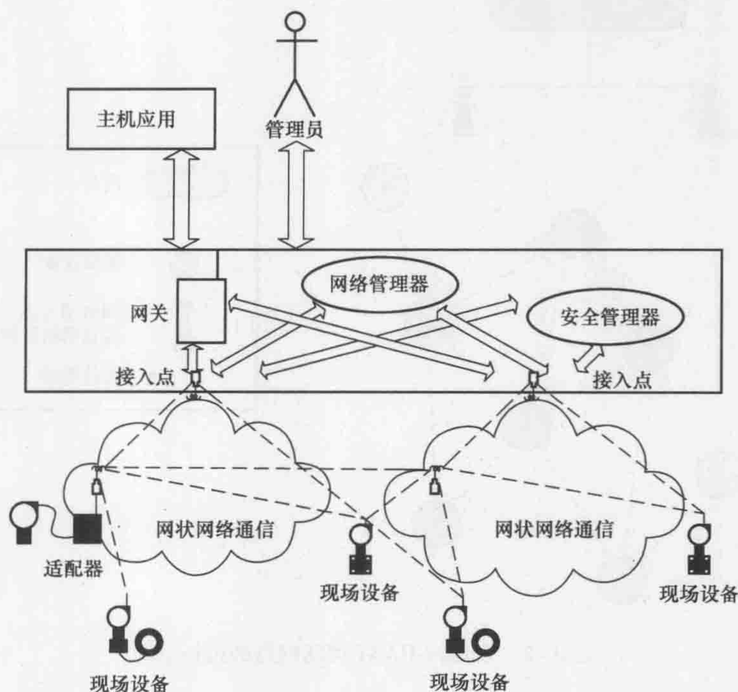


图 10-4　无线网络的网络结构图

因为数据传输的源设备与目标设备之间存在有多条冗余路径，所以网状网络拓扑结构提供了最健壮的无线网络拓扑结构。网状拓扑结构能够提供高的数据可靠性，这对于过程自动化工业来说是一个很关键的网络需求。图 10-5 描述了一个由多个网络设备组成的典型 WirelessHART 网络，这些网络设备都集成有实际工业现场仪表。

WirelessHART 网络管理器负责建立和维护一个网状网络。它确定最佳路由并管理时隙访问的分布（WirelessHART 把每秒分为多个 10ms 的时隙）。时隙访问取决于所需的过程值刷新率和其他一些访问（警报报告 - 配置改变）。如果由于一个障碍，网络路径变得不可靠或被破坏，那么 WirelessHART 网络管理器会自动为报文找到一条替代的路由路径。

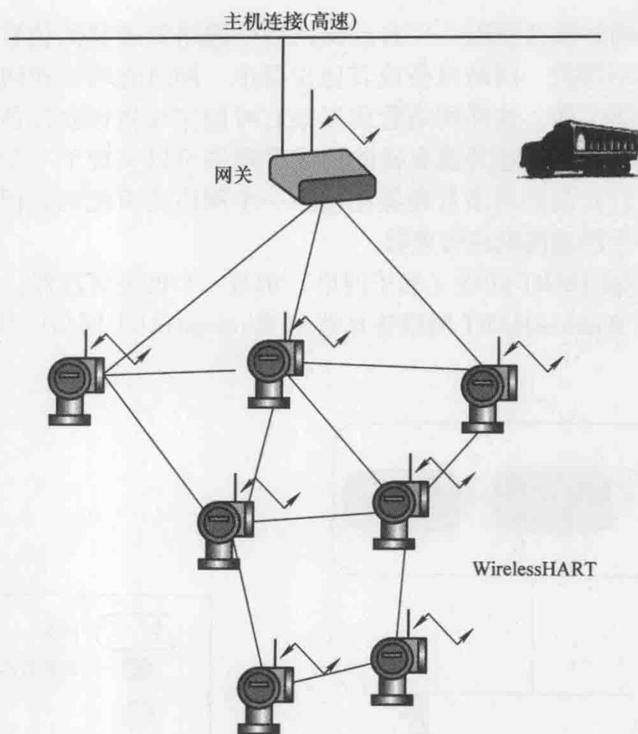


图 10-5　无线网络的网状拓扑图

10.4　WirelessHART 网络管理器

WirelessHART 网络管理器负责整个 WirelessHART 网络的管理、调度以及优化。作为其任务的一部分，网络管理器初始化、维护和管理网络通信的参数。网络管理器为设备入网和离开网络提供一些机制，并管理一些专用的和共享的网络资源。

网络管理器是一个应用程序，它以某种方式来协调 WirelessHART 网络和相关网络设备，从而确保工业应用所要求的服务质量。网络管理器执行以下一些功能：

1）形成一个星形或网状网络。

2）允许新设备连接到网络。

3）确定网络设备的最优通信调度。

4）为所有的通信建立冗余路由路径。

5）与安全管理器通信，对数据进行加密和认证以确保网络的安全。

6）实时监测网络的性能，并执行必要的改变以维持一个事先设定的服务

质量。

网状网络架构并没有限制工厂自动化网络中网络管理器的位置。网络管理器在物理上可以位于网关、网络设备或其他设备中。网络管理器和网关可以作为一个单一的逻辑实体工作，这样网络管理器最有可能实现将这些设备与网关搭配在同一物理框架内。然而，这并没有排除网络管理器可以实现于一个完全独立的物理设备。此外，让冗余的网络管理器连接到一个网络是可能的，但是每一个无线网络有且只有一个活动的网络管理器。

每一个 WirelessHART 网络（和子网络）都有一个网络管理器。图 10-6 是一个关系图，显示了 WirelessHART 网络管理器和 WirelessHART 网络中其余部分之间的关系。

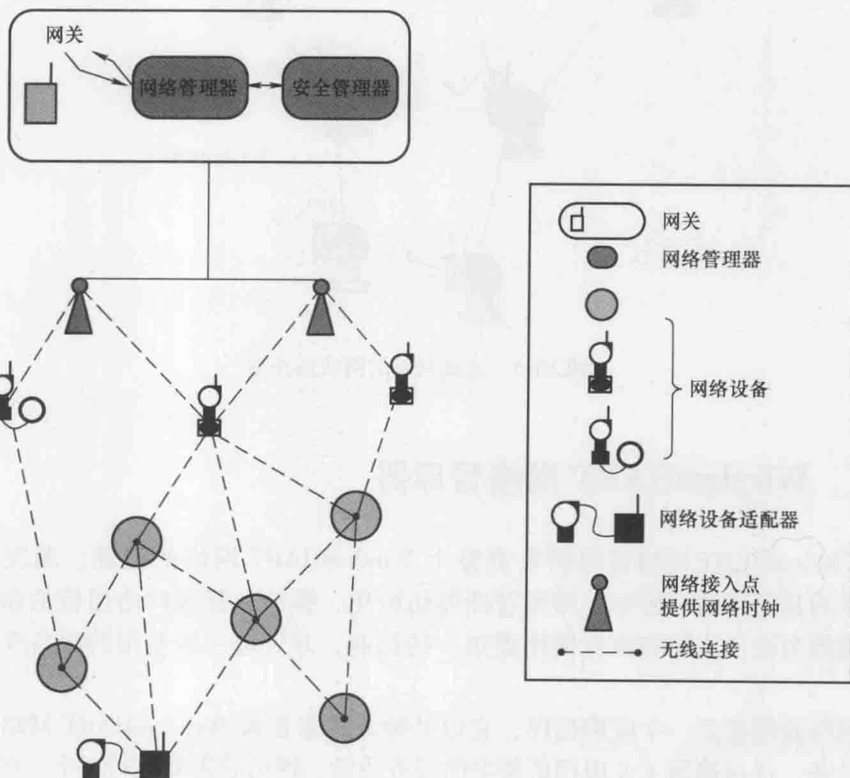


图 10-6　WirelessHART 网络中的网络管理器

网络管理器有一个固定的、公开的唯一地址，它被设置为 0xF980000001（16 位地址 = 0xF980），它被作为一个目的端，即从现场设备到网络管理器的应用层 PDU 的目的端。

网络管理器也负责收集和维护网络整体健康相关的诊断。这些诊断被报告给

基于主机的应用程序。这些诊断也被用于使整个网络适应不断变化的无线电频率环境，从而满足应用所要求的服务质量。

为了网络管理器能实现其完整的功能集，网络管理器需要关于网络设备的信息、网络是如何被使用的信息，以及来自于网络的关于网络执行效果的反馈。网络管理器可直接读取网络设备相关的配置和设置信息。网络设备、主机应用程序和工厂用户请求通信资源。关于网络执行效果的反馈由设备通过 WirelessHART 协议中的健康报告和诊断提供。

在这种情况下，网络管理器实时监测 WirelessHART 网络的任何性能改变。网络管理器收集以下的性能信息：

1）路径统计。

2）端对端可靠性。

3）信号强度。

4）电池寿命。

5）通信状态。

网络和路径性能在某条通信路径被阻塞时用于修复通信路径，或者发现冗余路径以防备通信问题。网络管理器中的优化算法使得 WirelessHART 技术具有自愈的特性，同时允许 WirelessHART 网络传递工业终端用户所要求的可靠数据通信。这种自动的自愈过程降低了工程投入，简化了 WirelessHART 的使用。

WirelessHART 标准没有规定网关和网络管理器之间的接口。然而，网络管理器和网关负责与对方建立一个安全连接，并维护此连接以实现控制信息和数据的通信。这样，网关就没有必要经过普通网络设备的入网过程。网关连接到网络管理器后，网络管理器可以配置网关，从而开始网络形成的过程。

10.4.1 网络结构

WirelessHART 网络的一个关键功能就是它的自我组织能力。网络管理器的这个功能，有四个关键要素：

1）公告。

2）入网。

3）调度。

4）发现。

1. 公告

作为公告机制的一部分，已经加入网络的设备将发送公告分组以宣示网络的存在。公告分组包括时间同步信息和一个唯一的网络标识符。欲加入网络的设备侦听这些分组，并尝试着将公告分组中的网络标识符与自己的网络标识符进行比对。当新设备侦听到至少一个公告分组时，新设备就可以尝试加入网络。

2. 入网

为了加入网络，新设备需要发送一个入网请求分组。该分组由入网密钥加密并包含有该设备的唯一 ID，并通过一个发送公告分组的节点传送至网络管理器和安全管理器。如果它被验证，那么网络管理器将响应一个激活分组，同时接受该新设备加入网络，并为该新设备与其他已存设备之间建立链路。此外，在验证后，网络管理器为网络设备分配合适的时隙和路由信息。

图 10-7 显示了一个报文序列图的例子，此图表示了一个网络设备在一个简单网状网络拓扑结构下加入 WirelessHART 网络的过程。此例描述了入网过程的细节。

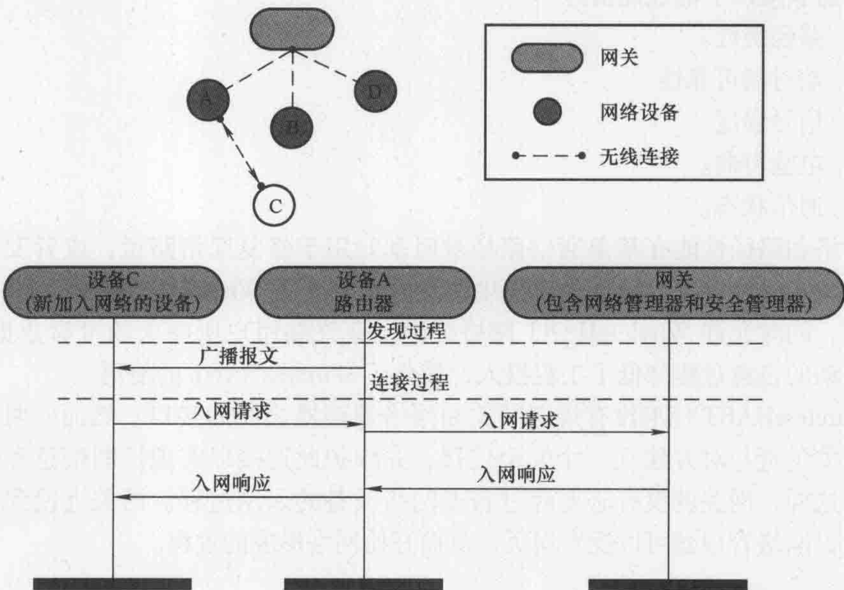


图 10-7 网络设备加入到 WirelessHART 网络的报文序列图

3. 调度

在新设备加入网络并被分配了初始通信资源（会话、超帧、链路等）后，该新设备会根据其被设定的发布率来请求额外的网络资源。网络管理器可以允许或否定这个网络资源的请求。如果网络管理器允许此请求，那么它发出一个调度给新设备以及任何与新调度信息相关的中间路由设备。当网关设备（通常在网络管理器有请求时）开始发送公告分组时，一个新的 WirelessHART 网络就开始了。作为网络中的第一个设备，网关开始它自己的调度，其他节点稍后也同步到此调度。调度允许网络设备定期报告和发布过程变量，或使得网关发出的命令得以到达对应的网络设备。图 10-8 显示的例子描述了一个网络设备发布过程信息的报文序列图。相似的，图 10-9 介绍了另一个报文序列图的例子，它描述了 WirelessHART 协

议中典型的命令响应报文序列图。

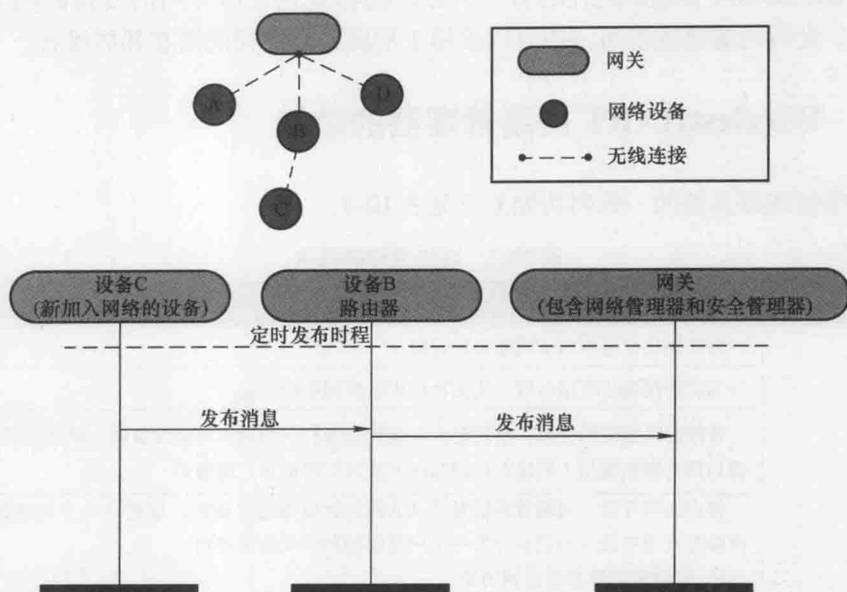


图 10-8　WirelessHART 网络中网络设备发布过程控制信息的报文序列图

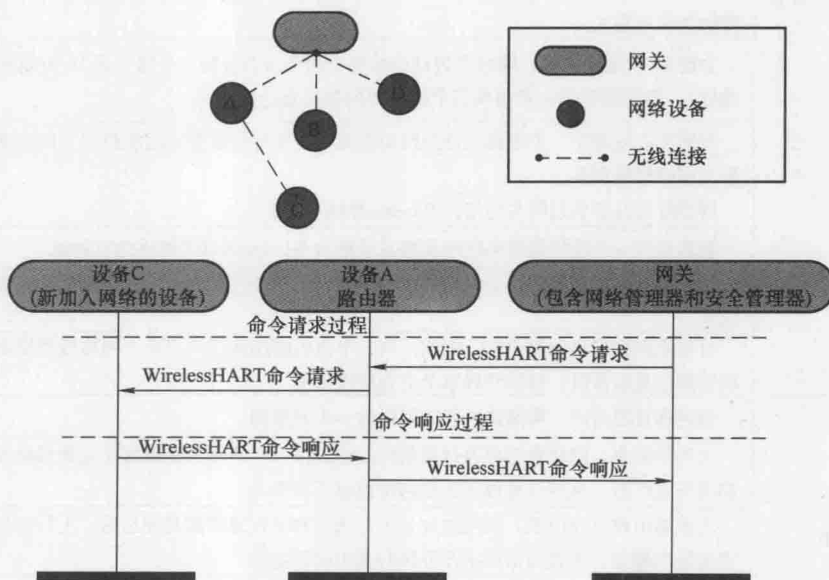


图 10-9　WirelessHART 命令请求/响应报文序列图

4. 发现

WirelessHART 自组织特性的另一个方面的特色是使用专用的发现时隙来发现新设备。此特色能够发现另一些可以被用于形成冗余路径的潜在邻居设备。

10.5 WirelessHART 网络管理器的功能

网络管理器具备的一系列功能汇总见表 10-1。

表 10-1　网络管理器需求

<table>
<tr><th>网络功能</th><th>需　求</th></tr>
<tr><td rowspan="11">网络信息和配置</td><td>为初始化自身和启动网络提供逻辑</td></tr>
<tr><td>当设备报告诊断信息时，使拓扑结构适应网络的变化</td></tr>
<tr><td>管理网络密钥的分发，密钥是由安全管理器提供给所有网络设备的。单独的网络管理器和网关密钥被用于网络管理器和网关发出的单播和广播通信</td></tr>
<tr><td>管理入网过程。网络管理器对尝试入网的新设备进行验证。在验证一个网络设备后，网络管理器应给入网设备分发一个网络密钥和四个会话密钥：
1）网络管理器单播会话密钥
2）网络管理器广播会话密钥
3）网关单播会话密钥
4）网关广播会话密钥
在新设备尝试加入网络之前，新设备应该被配置有网络 ID，以便它可以找到正确的网络来申请加入</td></tr>
<tr><td>分配 16 位地址昵称。网络管理器应给每个网络设备分配一个唯一的 16 位地址（网络地址）。网络管理器负责确保每个设备中的邻居表是最新的</td></tr>
<tr><td>与网关之间建立一个连接。每当网关收到一个发给网络管理器的报文，网关就转发该报文到网络管理器
网络管理器应通过网关连接到 WirelessHART 网络</td></tr>
<tr><td>配置至少一个连接到网关的网络接入点作为 WirelessHART 网络的时钟源</td></tr>
<tr><td>管理网络配置。维护一个完整的网络配置图，包括任何已经分发给网络设备的网络信息</td></tr>
<tr><td>对请求网络信息做出响应。例如，当一个主机应用程序使得某个网络设备发出一个网络管理信息请求时，网络管理器负责响应该请求</td></tr>
<tr><td rowspan="5">路由</td><td>创建和管理路由。网络路由代表网络的一个完整图</td></tr>
<tr><td>管理邻居表。网络管理器通过周期性的健康报告，从每个设备那里收集网络统计信息和邻居表信息。这些信息被用于使网络能够适应变化</td></tr>
<tr><td>为图路由建立路由表。图路由对于上行通信和下行通信都是理想的。上行通信包括过程测量和警报。下行通信包括改变执行器中的设定值</td></tr>
<tr><td>为源路由建立源路由列表</td></tr>
<tr><td>分配通信资源到网络设备、网关和网络管理器自身。这样，网络管理器就有分配的网络容量来管理网络，并且网络设备有足够的网络容量来相互通信</td></tr>
</table>

（续）

网络功能	需　求
网络调度	创建超帧。多个超帧被用于支持特定扫描速率的通信。额外的超帧将被分配用以支持设备管理和诊断应用，这种应用在短时间需要大量的通信
	分配超帧中的链路
	创建链路表。每个链路包括一个与某个超帧相关的时隙，链路的类型（普通链路、公告链路、发现链路），链路的选项（传送、接收、共享），邻居设备信息，信道偏移，以及与该链路相关的网络设备
	为响应应用需求，激活和停用超帧
信道管理	跟踪被列进黑名单的信道 注：将某个信道列到黑名单是一个手动操作过程
	提供信道偏移。信道偏移被用于在跳信道时计算信道数。信道偏移值的取值范围为 0 到（信道数减去被列进黑名单的信道数）
网络诊断和适应	维护全部无线网络诊断信息。如果一个网络设备在 Keep – alive – time 内还没收到来自于某个邻居设备的分组，那么该设备就发送一个"path – down"报文给网络管理器，以告知该路径不再可用
	维护每个网络设备的健康报告记录
	按网络设备请求分配通信资源。网络设备请求网络容量来支持数据发布，事件通知和块模式通信。网关请求网络容量来支持客户的要求。通过给某个特定网络设备增加或减少链路数量，网络通信可以偏向于某条特定路径
	优化路由和调度以提高网络的运作，同时可节省设备的功耗

10.5.1 智能更新

网络管理器可根据过程条件的变化而自动地改变其数据的发布率。这种功能被称为智能更新。这种机制可增强变化 RF 环境中通信的可靠性，扩大电池寿命，并允许特殊的通信通过。也就是说，不用主机应用程序的轮询行为（通过网关）来报告过程变量和状态。

图 10-10 显示了一个智能更新的例子，由一个过程变量的阈值触发。在这个例子中，当过程变量低于某个用户设定的阈值，其值需要以每 20s 一次的采样率进行采样（刷新）和通信。如果过程变量超过该阈值，那么一个时间标记的警报被生成并且采样（和通信）率被提高到每 10s 一次。

图 10-10 中的例子在过程变量从低到高跨过阈值时使用了一个触发器。智能更新也可设置为从高到低转换，并通过一个窗口触发机制。在这种情况下，过程变量被报告（发布）在两个可能触发事件之一：采样时间和过程变量值变化。图 10-11显示了窗口触发机制。

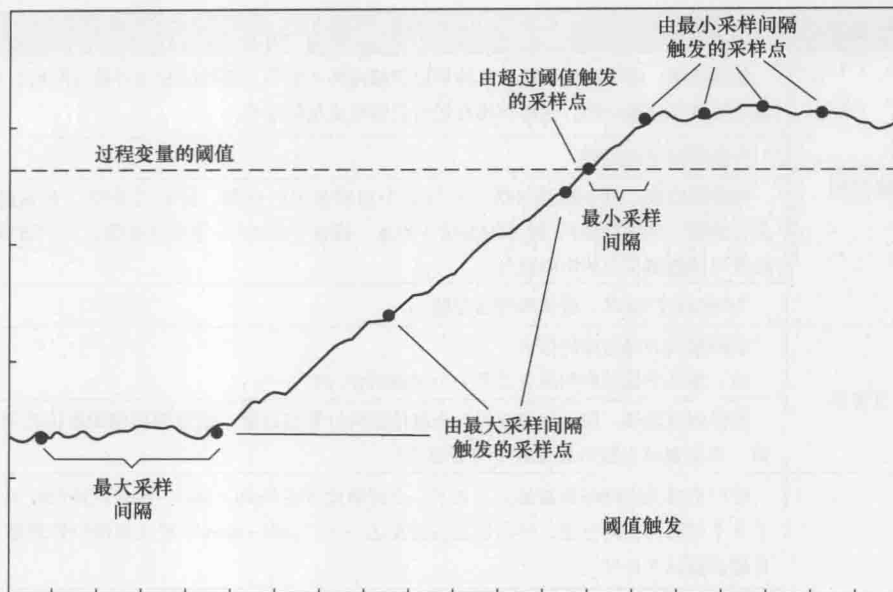


图 10-10　智能更新阈值触发

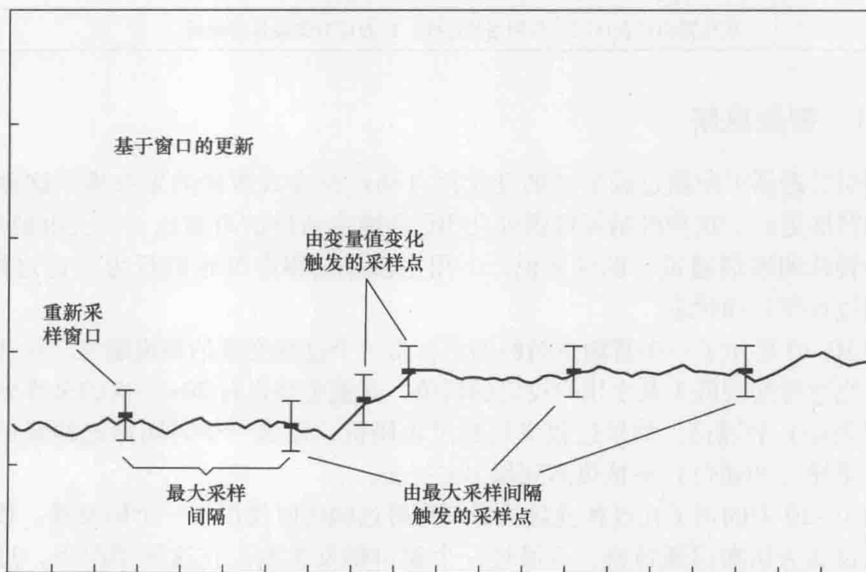


图 10-11　智能更新：窗口触发

注意，设备的采样将仍然以工业过程限定的更新率，但是只要没有到达触发，不是所有的采样值都会被传送。

WirelessHART 也定义了一个机制来允许对无线通信介质的非周期访问。此访问是由网络管理器通过一个特殊时隙——称为共享时隙来完成的。如果某个设备需要报告某个特殊的值（如报警），那么它等待下一个可用的共享时隙来传输此特殊值。

为了传输大量的过程信息，WirelessHART 规定一个增强的突发模式来有效地发布过程数据。突发报文被用来以在某个周期调度或特殊情况时发送数据。突发报文由指定命令的响应分组组成。突发模式率基于应用需要，是可配置的。

对于控制应用，突发模式率由控制回路或顺序执行需求（例如过程时间常数）决定。在某些情况下，不止一个主机应用程序将预定相同的发布数据。在这些情况下，更新率由最快数据请求率决定。

第 11 章　WirelessHART 物理层和数据链路层

WirelessHART 物理层利用 IEEE 802.15.4 – 2006 标准的 2.450MHz DSSS 物理层，它采用偏值四相移相键控（O – QPSK）调制。WirelessHART 物理层规定了信号编码方式、信号强度控制、设备灵敏度并管理 RF 参数来在无线介质中发送数据位。为确保符合国际规则，WirelessHART 规定了 RF 输出功率为 10dBm。

WirelessHART 物理层采用 IEEE 802.15.4 标准中的以下功能：

1）数据服务：发送和接收数据，在无线电频率介质上管理数字信息。

2）管理服务：管理本地参数，以控制物理层的操作，其中包括无线电操作的管理。

类似的，WirelessHART 数据链路层采用了 IEEE 802.15.4 标准的媒体访问控制机制。然而，为了达到低能耗的水平，WirelessHART 只利用了非信标模式，并将其与一个集中控制的时间同步超帧调度器相结合。

WirelessHART 标准采用了 IEEE 802.15.4 标准的强制功能，以及一部分可选功能。WirelessHART 数据链路层对 IEEE 802.15.4 标准中的 MAC 层功能进行了扩展和补充，同时还保持与 IEEE 802.15.4 标准的兼容。任何 WirelessHART 标准的实现都可以利用现有市场上各种商用 IEEE 802.15.4 设备（半导体收发机和 MAC 软件）。

11.1　WirelessHART 超帧

工业过程自动化网络（如 WirelessHART）要求严格的实时性和网状网，这就不允许使用 IEEE 802.15.4 标准提供的可选的 GTS 机制。

WirelessHART 超帧被定义为一个以某个固定速率重复的时隙的集合。不同于 IEEE 802.15.4 标准提供的可选的本地信标帧，WirelessHART 定义的超帧没有使用信标帧。由网络管理器控制的中央网络协调功能可以实现此功能。

一个时隙可以用来传输某个网络设备发出的过程自动化数据。WirelessHART 标准定义的时隙长度为固定的 10ms。

图 11-1 描述了一个 WirelessHART 超帧结构的例子。

WirelessHART 使用时分多路复用来最佳地利用时间和无线带宽。在 WirelessHART 超帧中，不是所有的时隙都是被分配的或是活跃的。网络管理器负责以最大化应用所要求的服务质量的方式，给所有网络设备分配时隙。例如，通过在多个信道上调度分配多个传输来实现时间的多样性。

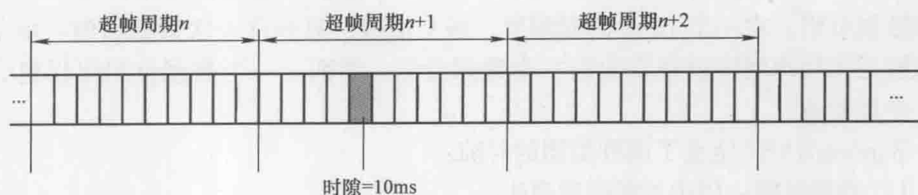


图 11-1 WirelessHART 超帧结构

不使用 IEEE 802.15.4 标准内置超帧结构的个人区域网（简称无信标网络），那么参数 macBea conOrder 和 macSuperframeOrder 都需要被设置为 15。在这种情况下，网络协调器将不会传送信标帧，除非它接收到一个信标请求命令。所有的传输，除了确认帧和在数据请求命令确认后的数据帧，都使用不分时隙的 CSMA - CA 机制来访问信道。

网络管理器中的优化算法设法避免 WirelessHART 网络中的 RF 碰撞，以及保持服务质量中的其他参数，如吞吐量和延迟。该优化算法在 WirelessHART 标准范围之外。厂商可以自由地创建自己的、适合于特定工业应用程序的最优网络管理器。

当网络设备加入 WirelessHART 网络时，它们根据设定的发布率来请求网络资源。网络管理器依据这些请求中的信息来分配和调度时隙，从而确保这些网络设备可以访问网络并且拥有需要的带宽来完成各自的任务。

即使当时隙长度为 10ms，WirelessHART 也允许定义来自于网络设备的批量数据传输或大块数据传输。大块数据传输通过将大块数据分割成多个小块数据，并将小块数据存放到可以传输的数据分组中，然后通过多个时隙来传送这些数据分组。工业过程自动化中大块数据传输的一个典型应用是振动传感器或分析化学传感器。

11.2 时分多址

WirelessHART 使用时分多址（TDMA）机制来协调通信，也就是说，它将时间分为有规律的时间间隔。此时分机制发生在 IEEE 802.15.4 标准定义的每个可用信道。

WirelessHART 利用 TDMA 机制来提供有序的、无碰撞的和确定性的传输，这种传输是在工业环境中所要求的。网络管理器集中管理着 TDMA 时隙分配和整个系统。网络管理器对终端用户应用程序隐藏了实时时隙管理的复杂性，并执行确定性的工业过程监测和控制。

通常，一个时隙被分配给两个设备——一个设备发送数据分组，另一个设备接收数据分组；在一个 10ms 的时隙里，每个信道上只允许一次数据通信。单个时隙只够用来处理网络设备发出的一个数据分组，然而，一个数据分组可以包含高达 8 个过程值。

WirelessHART 定义了两种类型的时隙：

1）专用时隙：用于过程变量报告。

2）共享时隙：用于传输特殊数据分组（如警报、事件），或在一些特殊情况下用于传输有规律的过程变量。

在每一次数据交换时，时间同步就会发生在数据链路层。时间同步的时间基准统一由网络管理器决定。

如果在一定区域内有多个 WirelessHART 网络，那么每个网络的网络管理器将彼此协调以实现多个 WirelessHART 网络的共存。此机制不在 WirelessHART 标准范围之内，但是可以通过协调相关网络管理器的时隙存量来轻易实现。

图 11-2 从发送方的角度展示了一个时隙是如何被建立的。空闲信道评估（CCA）在 10ms 信道的开始被执行。CCA 之后是实际数据分组的传输和相应的确认（ACK）的接收。

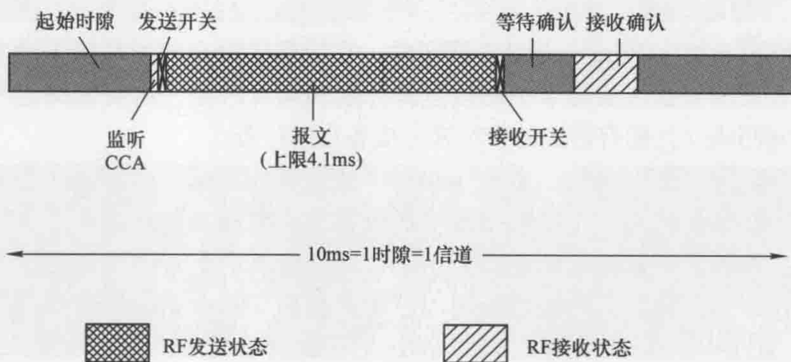


图 11-2　时隙结构总览图

在 WirelessHART 中，只有广播报文、公告报文和发现报文是不需要确认的。当从时钟源设备接收到一个数据分组或确认时，时间同步就实现了。时间同步通常依赖于有确认的数据传输。

图 11-3 显示了一个时隙，并提供了单次数据通信的时序。图 11-3a 显示了源网络设备（发送方）的操作，图 11-3b 显示了在目标网络设备（接收方）的操作。表 11-1 显示了时隙参数的详情以及对应的取值范围。所有 WirelessHART 数据报通信都要求严格符合这些时序参数的限制，这间接暗示了 WirelessHART 设备所需要

的时钟晶体精度比 IEEE 802.15.4 设备高许多。

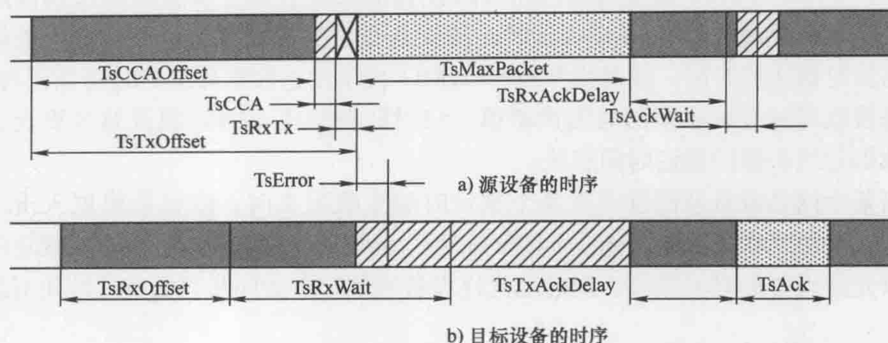


图 11-3　时隙的时序

表 11-1　时隙时序的定义和值

符号	描　述	需求值
TsTxOffset	从时隙开始到开始传送前报文中同步码之间的时间间隔	2120μs ± 100μs
TsRxOffset	从时隙开始到接收方必须开始侦听报文之间的时间间隔	1120μs ± 100μs
TsRxWait	等待报文开始的最短时间。该最短时间与邻居设备间在维持通信的前提下能容忍的偏移量有关	2200μs ± 100μs
TsMaxPacket	最长报文（包括物理层前同步码、定界符、长度和 DLPDU）所需的发送时间	4256μs
TsTxAckDelay	从数据报文的发送结束到确认报文开始之间的时间间隔。接收方必须确认数据传输的开始，并且在此期间产生一个确认报文 注意：广播报文不需要确认	1000μs ± 100μs
TsRxAckDelay	从数据报文的发送结束到发送方必须开始侦听确认报文之间的时间间隔	800μs ± 100μs
TsAckWait	等待确认报文开始的最短时间	400μs ± 100μs
TsAck	确认报文所占用的发送时间。值得注意的是：TsAck 可能根据所使用的寻址方式而变化，这样将导致 TsAck 的值分别为 800μs、992μs 或 1184μs	832μs
TsCCAOffset	从时隙开始到 CCA 开始的时间间隔	1800μs ± 100μs
TsCCA	CCA 的执行时间	128μs
TsRxTx	发送状态与接收状态之间的切换时间	192μs
TsError	报文的实际开始时间与接收方期望的报文开始时间之间的误差。换句话说，该值也可被认为是接收方与发送方之间的时间同步误差	

值得注意的是，源设备和目标设备的时隙开始时间由于时钟漂移的不同而可能不同。WirelessHART 设备利用与时钟源设备的每次数据交换就可补偿这些时钟漂移。当 WirelessHART 设备接收到时钟源设备发出的数据分组时，该设备就记录下数据分组抵达的时间。或者当 WirelessHART 设备发送数据分组给时钟源设备时，该设备接收到对应确认中的时间调整值。该时间调整值由时钟源设备计算出，并且与数据分组头部的抵达时间有关。

当某个网络设备被调度成在某个预定时隙接收报文时，该设备将进入接收模式。该设备将会在时隙开始的 TsRxOffset 延迟后开始侦听信道。TsRxWait 规定的接收窗口允许设备的时间漂移，同时也允许设备通信和重新同步它们的时隙定时器。

11.3　数据分组的传输

当发送数据时，网络设备在时隙开始后的 TsCCAOffset 段时间后执行一次时长为 TsCCA 的空闲信道评估（CCA）。如果该信道已被占用，那么该网络设备将在后续某个时隙被重新尝试发送数据。如果该信道是空闲的，那么该网络设备将收发器由接收模式转换到发送模式以发送 PPDU，这样，报文的开始（Start of Message，SOM）刚好发生于时隙开始后的 TsTxOffset 时间。

根据 WirelessHART 数据分组的类型，PPDU 可能会要求对其进行确认。如果这样，那么在 PPDU 传输之后会有一个确认等待时间（TsACKWait）和一个确认接收过程。

11.4　数据分组的接收

当接收数据时，网络设备在时隙开始 TsRxOffset 时间后进入接收模式，以侦听介质。网络设备持续不断地检查是否有报文抵达。如果在时隙开始后的（TsRxOffset + TsRxWait）时间内没有检测到报文，那么该网络设备将停止侦听。如果检测到报文，那么该网络设备将接收数据分组并对其进行验证。

在时隙的最后，一部分时间被用于处理接收到的数据分组并为下一时隙做准备（例如，评估在每个网络设备中排好队的数据分组和确定它的优先级）。如果其中一个邻居网络设备作为一个时间源，那么在一次成功的通信后，两个设备的时隙结束时间将变得齐整。为此，网络设备记录下物理层定界符开始的时间，并以此计算出时间误差（TsError，即物理层分隔符预期开始时间和实际开始时间的差值）。于是，网络设备就可以根据时间误差（TsError）来调整自己的时钟，从而实现与网络的时间同步。

11.5　确认通信

WirelessHART 网络中的大多数通信数据分组由以下两种数据分组组成：源设备发出的数据分组和目标设备发出的确认。对于带确认的通信，在数据链路层协议数据单元中的源端和目标端地址必须包含独立的设备地址。

如果接收到的数据分组是有效的，那么目标设备会检查数据链路层 PDU（DPDU）中的目标地址。如果该目标端地址不是一个广播地址而且没有接收错误，那么该目标设备将从接收模式转换到传输模式，并开始传输确认 PPDU。确认 PPDU 的报文的开始准时地发生于源设备发出的数据分组传输结束后的 TsTxAckDelay 时刻。

同时，源设备从传输模式转换到接收模式。在自己发送数据分组结束后的 TsTxAckDelay 时刻，源设备开始侦听信道，并在 TsAckWait 时间内监测确认的到达。

11.6　广播通信

WirelessHART 提供广播通信的功能。广播 DPDU 的源地址对应于报文发送方的源地址，而广播 DPDU 的目标地址被设置为广播地址（全部设置为 0）。网络设备在接收一个广播 DPDU 时，会对该数据分组进行验证并检查数据分组中的目标地址。如果目标地址是广播地址，那么该网络设备将不确认此广播 DPDU。

11.7　时间同步

整个网络的时间同步对于 TDMA 通信是必不可少的。然而，不管设备硬件时间源（例如，晶体、陶瓷谐振器等）的选择如何，由于温度、电压变化或老化，网络设备之间实际上会出现一些时间偏差。因此，WirelessHART 数据链路层采用几种机制来实现全网络时间同步。

当某个设备接收到一个发给自己的 DPDU 时，它将记录下该 DPDU 到达的时间。目标设备使用此信息计算出该 DPDU 实际到达时间和预期到达时间之间的差值（Δt）。该差值（Δt）被包含在每个 DPDU 的确认中，并发送给源设备。因此，每次带确认的通信都可用来确保设备之间的网络时间同步。

在某个网络设备的邻居设备列表中，网络管理器选择其中一个邻居设备作为该网络设备的时间同步源。当收到时间同步源发出的 DPDU 时，接收设备的网络时间会被调整。时间同步要么基于 DPDU 的到达时间，要么基于确认 DPDU 中的 Δt，这取决于是哪个设备发起此次通信的。

根据 WirelessHART 网络设备的时间漂移情况，WirelessHART 系统将要求调整其广播 Keep – alive DPDU 的频率；当时钟源设备有时间漂移时，设备根据需要传输 Keep – alive DPDU 到它的时间同步邻居，从而保持彼此间的时间同步。然而，当温度变化每分钟小于或等于 2℃时，设备发送一次 Keep – alive DPDU 的时间间隔应该被设置成大于或等于 30s。此外，设备应允许在分组丢失情况下的一次重试，这大约相当于一个百万分之十（10ppm）或更好的补偿时钟精度。值得注意的是，此准确度是差不多四倍于 IEEE 802.15.4 标准中规定的最小晶振偏差。

11.8 跳信道

跳信道技术与 TDMA 技术相结合以进一步增强网络的可靠性。图 11-4 描述了一个报文从网络设备到网关的传输，它使用了跳信道和 TDMA。

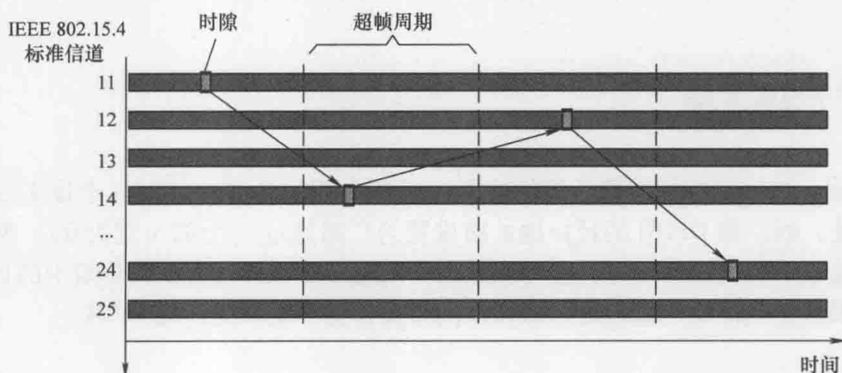


图 11-4　WirelessHART 跳信道机制

跳信道技术提供了频率的多样性，这可以有助于消除窄带干扰和减少多径衰落的影响。通过使用跳信道和 TDMA 技术，WirelessHART 网络可以提供工业环境所要求的高可靠性。

某个超帧、超帧内的某个时隙和某个信道偏移会被分配给某对通信设备。这三者形成了这对通信设备之间的通信链路。所有通信设备都能够支持多个链路。通常情况下，可能存在的链路数目等于网络可用信道数乘以超帧内的时隙数。例如，如果网络可用信道数为 15 个，每个超帧的时隙数为 9000 个，那么可能存在的链路数量为 135000 个。

跳信道提供了信道的多样性。因此，对于每个时隙，多个网络设备可以在不同的信道同时使用该时隙。这可以通过在相同的时隙上创建具有不同信道偏移的链路来具体实现。每个网络设备维护一列正在使用的信道以及信道对应的参数

(如频率)。所有网络设备都具有相同的、由网络管理器确定的信道列表。网络管理器负责网络中所有设备的链路的动态分配。

WirelessHART 也支持信道黑名单，也就是说，WirelessHART 允许网络管理器对网络设备所使用的跳信道技术进行限制，使得跳信道技术仅使用某个 RF 频段内选定的某些信道。例如，网络管理员可以将某些信道列为黑名单，以限制使用某些固定 RF 频段的无线服务，因为此 RF 频段可能已经在这个网络中被其他一些网络设备占用。实际上，对于使用其他协议的设备，其在某个可用带宽上的通信是很随机的，并且只使用总可用带宽中的很少一部分。因此，黑名单技术很少能提供实实在在的好处。

第12章　WirelessHART安全

正如在前面章节所强调的，安全在无线通信系统中是一个主要问题。在WirelessHART中，通信安全涉及了WirelessHART堆栈中多个协议层。WirelessHART技术在确保易于使用的同时，是为安全工业无线传感器网络通信而设计的。WirelessHART通过以下多个机制来保证工业无线传感器网络通信的安全：

1）安全功能是内置的且不能被禁用；安全功能总是有效的。

2）标准AES－128位加密。

3）密钥管理机制。

4）端到端安全；只有最终接收设备可以解密和使用由源设备创建的数据有效载荷。

5）通过使用由跳信道技术所带来的频率多样性，可以减少服务攻击的拒绝。

6）通过使用报文完整性检查和维护一个相关网络设备的白名单，可以消除欺骗。

7）使用内置的IEEE 802.15.4标准安全引擎（报文更新）和TDMA技术来处理重放攻击。

图12-1显示了WirelessHART实现的安全体系架构。WirelessHART安全体系架构被设计成有助于工厂操作员最小化、控制和审核网络访问，只有高水平的技术专家才有可能破坏网络。此外，WirelessHART安全模式的定义方式是尽可能减少任何独立安全缺口所导致的安全后果（跨度和持续时间）。

为防止窃听，安全管理器为WirelessHART网络提供了基础设施以执行设备的安全入网、设备认证和报文加密。入网密钥和网络ID被用来对入网设备进行验证。此外，安全管理器可以采用一个设备白名单（即其期望加入网络的设备）或设备黑名单（即其禁止加入网络的设备）来支持设备认证过程。上述机制中的最后一个机制［即使用内置的IEEE 802.15.4标准安全引擎（报文更新）和TDMA技术来处理重放攻击］可被用来防止克隆设备加入网络。

作为正常的网络异常活动监测的一部分，安全管理器维护消息完整性代码失效、认证失败和入网尝试失败的统计数据。安全管理器可以在这些统计数据的基础上产生警报并报告，以表示网络活动的不同状态。

安全管理器监测以下异常网络活动：

1）加入网络失败。

2）过多的重传。

3）消息完整性代码（MIC）失效。

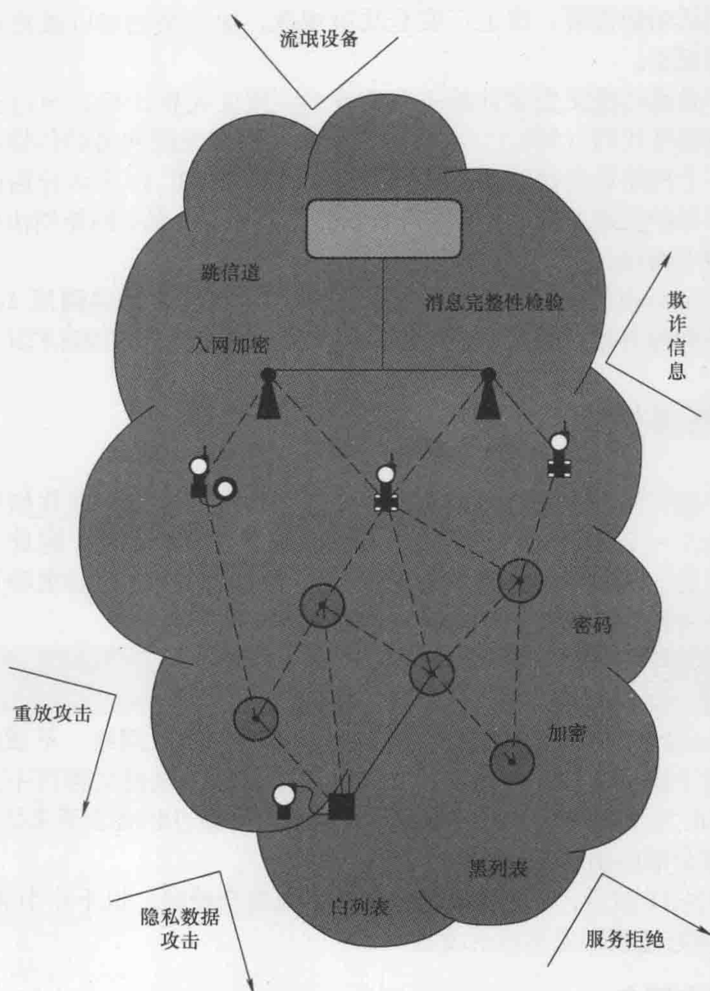


图 12-1 WirelessHART 安全机制

4）认证失败。

网络设备没有被授权作为网络密钥服务器或无线网络管理器，这最大限度地减少了黑客利用手持设备来攻击网络的机会。此外，WirelessHART 不使用 TCP/IP 通信栈，所以许多互联网上常见的黑客工具和黑客攻击对于 WirelessHART 而言则无用武之地。因此，WirelessHART 显然是安全的。

12.1 数据保护和保密

数据保护和保密负责维护网络数据的私密性和完整性。WirelessHART 网络在从数据源到数据消费者的网络/传输层，提供端对端 CCM* 模式 AES－128 位加密。除了私人会话密钥，WirelessHART 网络中的所有设备都共享一个共同的网络密钥，

从而满足广播活动的需要。按工厂安全政策规范，加密密钥可以被更新以提供一个更高水平的保护。

数据保护是通过报文完整性检查来实现的。报文完整性检查通过分析每个分组中的消息完整性代码（MIC），来检查该分组在整个无线网络的传输过程中是否被改变。当一个网络设备接收到一个分组时，它检查 MIC 以确认分组的内容没有被修改。除了保护无线 PPDU 的数据有效载荷外，MIC 也保护网络路由信息，防止试图改变分组中网络/传输层信息的攻击。

总之，WirelessHART 有一个共享的网络密钥，用于数据链路层 MIC 的生成。每个广播会话都拥有相应的共享的广播密钥，用于有效载荷的加密和认证。

12.2　网络保护和可用性

网络保护和可用性，负责在面对内部和外部攻击（故意的或非故意的）时维护网络的运作。一个无线网络的覆盖范围可以超出工厂的区域，因此对于外部实体来说是开放的。从网络保护的观点来看，包括仪器仪表在内的现场设备都不能提供新的加密密钥，只有安全管理器才能提供此服务。

WirelessHART 不使用 TCP/IP，因此免受因不断发展的互联网协议黑客工具所引起的攻击。

在 WirelessHART 中，只有被信任的设备才被允许加入网络。不被信任的通信会被视为来自干扰设备；如果某个报文验证失败，那么该报文将得不到确认并且接收到的 PPDU 也会被丢弃掉。所有的端到端通信都通过私有会话来处理。只有终端设备才知道会话密钥。

WirelessHART 被设计成处理所有已知的无线安全威胁。以下小节将总结 WirelessHART 如何处理最常见类型的攻击。

12.2.1　拒绝服务

当网络因大量的数据分组或网络命令（例如入网请求）而中止运行时，无论这种情况是故意的或非故意的，拒绝服务都会发生。这样，正常的通信就无法发送到其目标地。WirelessHART 通过限制入网请求的可用带宽来处理拒绝服务攻击，这样上述类型的网络泛洪将不会对网络产生影响。此外，MIC 不正确的数据分组将被丢弃且不在网络中传播。

最后，网络管理器维护一个通信统计信息，并可以报告各种异常活动，以及当某个攻击设备处于网络设备附近时发出网站安全警报。

12.2.2　重放攻击

网络层中的随机数（Nonce）与时隙数相关，这样常规的重放攻击就不起作用了。倘若有某个重放攻击事件，网络管理器将报告异常网络活动，并直接给网站

安全发出一个警报。此外，随机数（Nonce）也被用于数据链路层的 MIC 中，从而在该层提供了另一级别的保护以防止重放攻击。

在网络层的重放攻击不能被可靠地报告。如果由于干扰等原因导致确认包没有被接收到，那么 WirelessHART 的网状结构可能会导致一些数据报的复制。因此，只有过多的重放攻击才可以被报告。

12.2.3 克隆设备

克隆设备使用其他设备的认证信息来渗透到网络。为此，一个克隆设备需要三个关键信息：

1）被克隆设备的唯一标识符（UID）。

2）一个网络设备 TAG。

3）入网密钥。

一个克隆设备可能可以得到 UID 和设备 TAG，但是它很难获得入网密钥，因为安全管理器会周期性的更新入网密钥。即使安全管理器不更新入网密钥，此密钥也是一个不能从设备检索到的只写参数。

12.3 安全管理器功能

安全管理器根据设备 UID、网络 ID、设备 TAG 和入网密钥来验证新设备。它也验证报文，以确保它们在通过无线网络时没有被改变。

WirelessHART 安全管理器负责以下加密密钥的生成、保存和管理：

1）入网密钥。

2）网络密钥。

3）会话密钥。

入网密钥提供一个安全的方法来添加一个新设备到网络。它可以是一个固定的密钥，或者是一个对于每个被添加设备来说都不同的密钥。终端用户在设定安全程序时可对此做出自己的选择。

入网密钥不在空中传输，而是通过本地物理连接（即设备的 HART 接口）传输。采用这种方式的理由是为了防止窃听。

会话密钥被用于加密一对会话之间的报文，这样最终目标设备可以解码和使用由源设备创建的有效载荷。

网络密钥被作为一个共同的网络加密密钥。网络密钥被所有网络设备共享，且可以被修复或更新以提供一个更高级别的安全。网络密钥也被用于生成 DPDU 的 MIC，从而验证数据链路层的数据报，帮助检查数据报的完整性。

第13章　结　束　语

距离IEEE 802.15.4标准组成员第一次相遇已经有超过10年的时间了。时间见证了一个围绕无线物联网的新行业的创立，这使机器对机器的通信成为了可能。正如当初所计划的一样，ZigBee联盟组织成为了使用IEEE 802.15.4标准的一个主要平台，它使IEEE 802.15.4标准用于住宅、商业和消费电子应用。类似的，HART通信基金会是无线传感器网络应用于工业领域的催化剂。同时，IEEE 802.15.4团体正在继续成长，通过制定一些最初标准的修订版来使得该标准可被专业化用于某些特定地区或某些特定等级的应用。

很难预测无线传感器网络以后的十年会怎么样。这个行业的成长将与很多主要应用（比如智能电网、工业过程控制和家庭自动化）的成功有很大的关系。更有可能的是，一些新的专有领域，比如楼宇自动化，将变得非常突出。

另外一个因素是其他无线技术正在试图加入到无线传感器网络领域。低功耗Wi-Fi和蓝牙芯片组被用于支持无线传感器网络应用。如今它们的低功耗模式中的功耗仍然比现有的成熟的IEEE 802.15.4芯片组的功耗要高一些，但相比于几年前功耗已经降低了很多了。按照这个趋势进行推断，我们很容易发现除非IEEE 802.15.4技术加速其在其预期市场的投入，不然我们会在市场内看到一些有趣的变化。

IEEE 802.15.4标准被设计用于满足只要求适当的数据吞吐量、很低的功耗、很低的实现成本的应用领域的需要。IEEE 802.15.4标准的设计者致力于制定出一个能满足大范围应用需求的标准（如从用于智能农业和军用应用的无线传感器网络、到工业控制和监测网络、再到消费电子和家庭自动化使用），同时保持少量代价高的选项和很少被使用的特殊功能，同时可以为某个应用最优化性能。IEEE 802.15.4标准的创立者相信，专业化和复杂性之间的合适平衡会最大化该标准的应用领域。

对于系统架构师和决策者，一个重要的策略就是：他们的开发总是针对用户需求和相关的应用要求，然后选择能更好满足这些需求和要求的正确的技术——在对某个应用有一个完整定义之前不要选择技术。换句话说。IEEE 802.15.4标准不是一个万能的解决方案，而是一个针对多种应用的通用平台。

词 汇 表

访问控制列表（ACL）：被某一设备用于决定哪些设备被授权执行某一特定功能的表格。

自组织网络：由通信设备组成的一个无线网络，且无须依靠已经存在的基础设施。一个自组织网络通常是通过一种自发的方式创建的，且是自组织和自我维持的。

适配器：在两个不同通信协议之间提供物理和逻辑连接的设备。

高级加密标准（AES）：由美国政府在联邦信息处理标准（FIPS）197 中所规定的对称加密算法（http：//csrc. nist. gov/encryption/aes/）。

应用层：开放系统互连（OSI）数据通信模型中的最高层，在应用层中执行应用功能，且会直接影响终端用户。

连接：被用于在一个无线个域网中建立成员之间关系的一种服务。

身份认证：被用于鉴别一个设备是否是一个设备集合中的一个成员的服务，该设备集合中的设备可以被允许安全地与该集合中的其他设备进行通信。

可靠数据：可以通过加密方式核实其来源的数据。

带宽：一个通信信道的最高频率和最低频率之差。更通俗地说，就是在一个通信信道上每次能够传送的最多的数据。

基带：一个通信信道，通过此信道可以不改变频率（例如，调制一个高频载波）发送一个恒压符号（例如，直流电压）；在信号调制载波之前由该信号所占用的频带。

波特率：对信号速度的度量，等于每秒内离散条件或事件的数目；在一个通信系统中每秒传输的符号数。

比特率：对通信系统中每秒的信息数量的度量；也是通信系统中每秒内的二进制符号数。

蓝牙：由蓝牙特殊兴趣小组（http：//www. bluetooth. org）创办的一个无线个域网规范，并被标准化为 IEEE 802. 15. 1。

宽带：与一个参照物相比有一个很大的带宽；特别地，一个调制过的信号和与它相关联的基带信号相比，有更大的带宽。更通俗地说，是一个适用于多媒体应用的高比特率。

信道跳频：用于为 DSSS 系统提供频率多样性的技术。该技术帮助消除带内干扰和减少多径衰落的影响。

空闲信道评估：在传送数据之前评估通信信道，以确定信道是否被占用。

保密性：保证通信数据的隐私性。

协调器：拥有网络设备功能的全功能设备，也能通过传送信标来提供设备的同步以及创建一个超帧结构。如果一个协调器是 PAN 的主控制器，那么它被称为 PAN 协调器。

覆盖域：两个或更多的 IEEE 802.15.4 标准单元交换信息的区域。

循环冗余检验（CRC）：与数据块一起传送的错误检测代码，目的是检查数据的错误。

数据完整性：确保收到的数据没有被修改，还是其原始形式。

数据链路层：在计算机系统之间用于通信的开放系统互连参考模型中物理层和网络层中间的那一层。

断开连接：解除一个已经存在的连接服务。

电子设备描述语言（EDDL）：一个基于文本的、特定领域的语言，通常被用在工业应用中来描述现场设备的性能。

帧：来自 MAC 层实体的、被一起实时传输的聚合的比特格式。

全功能设备（FFD）：能够以一个协调器或网络设备来运行且能够实现完全的协议设置的设备。

网关：连接无线网络和回程网络的设备，它允许数据在两个网络之间传输。

IEEE：参见"电气电子工程师学会（IEEE）"。

IEEE 802.11 标准：一种 IEEE 标准，为本地区域中的固定的、便携的、移动设备之间的无线连接，规定了媒体访问层和物理层规范，其数据速率是 1Mbit/s 和 2Mbit/s。

IEEE 802.11a 标准：IEEE 802.11 标准的延伸，使用正交频分复用（OFDM）技术调制，运行在 5GHz 频带，数据速率高达 54Mbit/s。

IEEE 802.11b 标准：IEEE 802.11 标准的延伸，在 2.4GHz 频带使用直接序列扩频技术调制，数据速率高达 11Mbit/s。

工业、科学和医疗（ISM）频段：为国际协定所允许的应用而保留的无线电频带。与 WPAN 相关的 ISM 频段是 900MHz、2.4GHz 和 5.7GHz。

电气电子工程师学会（IEEE）：一个非营利性的技术专业协会，目标是通过促进技术创新来推进全球繁荣，促进全球交流。IEEE 推进了工程过程的创建、开发、整合、共享，并运用与电子信息技术和科学相关的知识来造福人类和他们的职业（http://www.ieee.org）。

完整性代码：使用对称密钥生成的数据字符串，通常是附加到数据上以提供数据的完整性和来源的身份验证（也称为消息完整性代码）。

国际电工委员会：国际电工委员会（IEC）是一个国际化组织，它为所有的电力、电子和相关的技术进行编导和发布国际标准。

国际标准化组织（ISO）：一个在世界范围内，非政府组织的国家级标准机构，

促进标准化的发展及相关活动以促进国际商品的交换和服务，并在知识、科学、技术和经济活动领域发展合作（http：//www. iso. org）。

国际电信联盟（ITU）：联合国机构中的一个国际组织，在这里政府和私营部门协调全球的通信网络和服务（http：//www. itu. int）。

ISO：参见“国际标准化组织（ISO）”。

ITU：参见“国际电信联盟（ITU）”。

密钥建立：两个实体安全地创建一个对称密钥的过程，此密钥只有参与实体知道。

密钥管理：在其整个生命周期内控制密钥材料的方法，包括创建、分配和破坏。

密钥传输：一个实体发送密钥到另一个实体的过程。

ISM 频段：参见“工业、科学和医疗（ISM）频段”。

逻辑信道：物理通信链路上不同信道中的一个。

逻辑链路控制子层：OSI 参考模型中数据链路层的上层，负责数据流的组织。

低速无线个域网（LR－WPAN）：一个无线个域网，优化了低数据率应用，强调电池寿命长、低实现成本。

MAC 子层：参见“媒体访问控制子层（MAC 子层）”。

MAC 协议数据单元：在两个媒体访问控制实体之间交换的数据单元。

媒体访问控制子层（MAC 子层）：开放系统互连（OSI）参考模型中数据链路层的下层，负责获得权力来使用底层物理通信介质。

信息完整性代码：参见“完整性代码”。

移动设备：在移动中使用网络通信的设备。

窄带：与一个参照物相比有一个很小的带宽；特别地，一个调制过的信号和与它相关联的基带信号相比，有更小的带宽。更通俗地说，一个适用于声音和数据应用的低比特率。

网络接入点：在无线网络和网关间提供互连的设备。

网络设备：一个精简功能设备（RFD）或全功能设备（FFD），包含到无线介质的 IEEE 802. 15. 4 标准的媒体访问控制和物理接口。

网络层：开放系统互连（OSI）参考模型中数据链路层和传输层的中间层，为计算机系统之间的通信提供路由和转换功能和过程。

网络管理器：专用于配置和优化 WirelessHART 网络的设备。

网络拓扑结构：网络的逻辑结构。

开放系统互连（OSI）：计算机系统之间（可能是异构的）通信的 7 层 ISO 模型结构。

孤点设备：一个失去了与它相关联的个人局域网协调器的连接的设备。

分组：通过物理介质一起实时传输的格式化的聚合比特。

PAN协调器：一个协调器，是一个个人局域网的主控制器。一个IEEE 802.15.4标准网络只有一个PAN协调器。

父节点：与一个网络设备相关联的PAN协调器或协调器。

有效载荷数据：一个被传送的数据消息的内容。

有效载荷保护：为有效载荷数据提供安全服务的通用术语，包括保密性、数据完整性和身份验证。

对等网络：一个显著的同构网络，在其中设备平等地交流，经常采用分布的、多跳路由协议。

个人局域网（PAN）：一个个人操作空间的无线网络。

个人操作空间：关于一个人或物体的空间，通常是指在所有方向10m范围以内，并包络着不论运动与否的人或物体。

物理层：开放系统互连（OSI）参考模型中数据链路层的下一层，为计算机系统通信里的数据链路实体之间提供物理连接。

便携式设备：一种可以从一个位置移动到另一位置的设备，但是在一个固定位置时只使用网络通信。

协议数据单元：在两个对等实体之间进行交换的数据单元。

伪随机数生成：从一个给定的种子生成一个确定性的位序列的过程，当种子是未知时，它拥有一个随机位序列的统计特性。

随机数字生成器：提供一个不可预测的位序列的设备。

精简功能设备：仅具备IEEE 802.15.4标准中一部分功能的设备，且只有网络设备所具有的功能。

安全管理器：在WirelessHART网络中专门用于创建、存储、分配和管理加密密钥的设备。

安全套件：被设计用来在MAC层帧上提供安全服务的安全操作。

服务接入点：提供到服务接口的访问的任何实体。

服务数据单元：通过服务接入点的一个单元所传递的信息。

服务原语：在一个通信协议各层之间所提供的服务基本单元。

星形网络：一个使用了单一的中央设备的网络，所用设备之间的通信都必须通过该中央设备。

对称密钥：在两个或更多的实体之间所共享的一个秘密密钥，它可以根据它的用途用于加密/解密或者完整性保护/完整性验证。

时分复用（TDM）：使用这种技术，两个或两个以上的信号或数据流可以同时在一条通信线路上传输，其表现为同一通信信道的子信道，时隙被分为一些小段，每段时隙长度是固定的，每段时隙用于传输一个子信道。

事务：两个对等的媒体访问控制（MAC）实体之间相关的连续帧的交换，需要成功地传输一个MAC命令帧或数据帧。

传输层：开放系统互连（OSI）参考模型中网络层和会话层中间的一层，在会话实体间提供透明的数据传输。

无线本地局域网（WLAN）：一个计算机通信网络，跨越最多是校园大小（1km）的区域，使用无线电、红外或其他无线物理介质。

无线介质（WM）：在低速无线个域网（LR - WPAN）的对等物理层（PHY）实体之间，用于实现协议数据单元传输的介质。

无线城域网（WMAN）：一个计算机通信系统，跨越最多是城市大小的区域，使用无线电、红外或其他无线物理介质。

无线个人局域网（WPAN）：一个计算机通信系统，跨度是个人操作空间，使用无线电、红外或其他无线物理介质。

ZigBee 联盟：一个由多个公司组成的协会，致力于创造一个非常廉价、极低功耗、双向、无线通信的标准。

参考文献

[1] Braley, Richard C., Gifford, Ian C., and Heile, Robert F., "Wireless Personal Area Networks: An overview of the IEEE P802.15 working group," *ACM Mobile Computing and Communications Review*, vol. 4, no. 1, January 2000, pp. 26 – 34.

[2] Callaway, Ed, Bahl, Venkat, Gorday, Paul, Gutiérrez, José A., Hester, Lance, Naeve, Marco, and Heile, Robert, "Home Networking with IEEE 802.15.4, a Developing Standard for Low – Rate Wireless Personal Area Networks," *IEEE Communications Magazine*, special issue os Home Networking, vol. 40, no. 8, August 2002, pp. 70 – 77.

[3] Craig, William C., "ZigBee: Wireless Control That Simply Works," ZigBee Alliance white paper.

[4] Ennis, G., "Impact of Bluetooth on 802.11 direct sequence," *IEEE P802.11 – 98/319*, 1998.

[5] European Conference of Postal and Telecommunications Administration (CEPT), European Radiocommunications Committee; Relating to the Use of Short Range Device (SRD). CEPT/ERC/REC Recommendation 70 – 03. December 2002.

[6] European Telecommunication Standards Institute, Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1000 MHz frequency range with power levels ranging up to 500 mW; Part 1: Technical characteristics and test methods. ETSI EN 300 220 – 1 V1.3.1. Sophia – Antipolis, France: European Telecommunication Standards Institute, September 2001.

[7] European Telecommunication Standards Institute, Electromagnetic Compatibility and Radio Spectrum Matters (ERM); Wideband Transmission Systems; Data Transmission Equipment Operating in the 2, 4 GHz ISM Band and Using Spread Spectrum Modulation Techniques. ETSI EN 300 – 328. Sophia – Antipolis, France: European Telecommunication Standards Institute. 2001.

[8] Gutiérrez, José, Naeve, Marco, Callaway, Ed, Bourgeois, Monique, Mitter, Vinay, and Heile, Robert F., "IEEE 802.15.4—A Developing Standard for Low – Power, Low – Cost Wireless Personal Area Networks," *IEEE Network Magazine*, vol. 15 no. 5, September/October 2001, pp. 12 – 19.

[9] Heegard, Chris, Coffey, John (Seán) T., Gummadi, Srikanth, Murphy, Peter A., Provencio, Ron, Rossin, Eric J., Schrum, Sid, and Shoemake, Matthew B., "High – performance wireless ethernet," *IEEE Communications*, vol. 39, no. 11, November 2001, pp. 64 – 73.

[10] Howitt, I., "Bluetooth performance in the presence of 802.11b WLAN," *IEEE Transactions on Vehicular Technology*, vol. 51, 2002.

[11] Howitt, I., "WLAN and WPAN Coexistence in UL Band," *IEEE Transactions on Vehicular Technology*, vol. 50, 2001, pp. 1114 – 1124.

[12] Howitt, I., and Gutiérrez, J. A., "IEEE 802.15.4 low rate wireless personal area network coexistence issues," *Proceedings of the WCNC 2003*, 2003.

[13] Howitt, I., Mitter, V., and Gutiérrez, J., "Empirical study for IEEE 802.11 and Blue-

tooth interoperability," *IEEE Spring VTC 2001*, Rhodes, 2001.

[14] IEEE Std 802.11™—1999, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[15] IEEE Std 802.15.1™ - 2002, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs).

[16] IEEE Std 802.15.4 - 2003, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low - Rate Wireless Personal Area Networks (WPANs).

[17] International Electrotechnical Commission, IEC 62591 ED.1 International standard—Industrial communication networks—Wireless communication network and communication profiles—WirelessHART™, April 2010.

[18] Karaouz, Jeyhan. "High - rate Wireless Personal Area Networks," *IEEE Communications*, vol. 39, no. 12, December 2001, pp. 96 - 102.

[19] Marks, Roger B,. Giffod, Ian C,. and O'Hara, Bob, "Standards in IEEE 802 unleash the wireless internet," *IEEE Microwave*, vol. 2, no. 2, June 2001, pp. 46 - 56.

[20] O' Hara, Bob, Petrick, Al, *IEEE 802.11 Handbook: A Designer's Companion*. New York: Standards Information Network, IEEE Press, 1999.

[21] Poor, Robert D., *Embedded networks: Pervasive, low - power, wireless connectivity*, Ph. D dissertation, 2001, Massachusetts Institute of Technology, Cambridge, MA.

[22] Schwetlick, Horst and Wolf, Andreas, "PSSS—Parallel Sequence Spread Spectrum Application in RF communication," Proceedings from the *International Symposium on Signals, Systems, and Electronics (ISSSE)* 2004.

[23] Siep, Tom, *An IEEE Guide: How to Find What You Need in the Bluetooth™ Spec*. New York: Standards Information Network, IEEE Press, 2000.

[24] Siwiak, Kai, *Radiowave Propagation and Antennas for Personal Communications*, 2nd ed., Boston: Artech House. 1998.

[25] U. S. Code of Federal Regulations, vol. 47, sec. 15.247. Washington, D. C.: U. S. Government Printing Office. 2001.

[26] U. S. Code of Federal Regulations, vol. 47, sec. 15.249. Washington, D. C.: U. S. Government Printing Office. 2001.

[27] U. S. Department of Commerce, National Institute of Standards and Technology, Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips - 197.pdf.

[28] van Nee, Richard, "A new OFDM standard for high rate wireless LAN in the 5 GHz band,"

Proc. IEEE Veh. Tech. Conf., 1999, vol. 1, pp. 258 - 262.

[29] Zimmermann, Hubert, "OSI reference model—The ISO model of architecture for Open Systems Interconnection," *IEEE Trans. Commun.*, vol. COM - 28, no. 4, April 1980, pp. 425 - 432.

[30] Zyren, J., "Reliability of IEEE 802. 11 Hi rate DSSS WLANs in a high density Bluetooth environment," *Bluetooth'99*, 1999.

[31] http://www. zigbee. org

[32] http://www. hartcomm. org

[33] http://www. isa. org

[34] http://www. ietf. org/html. charters/6lowpan - charter. html

国际视野　科技前沿

国际信息工程先进技术译丛

《低速无线个域网：实现基于IEEE 802.15.4的无线传感器网络（原书第3版）》
《6LoWPAN：无线嵌入式物联网》
《虚拟网络——下一代互联网的多元化方法》
《下一代融合网络理论与实践》
《认知视角下的无线传感器网络》
《移动云计算：无线、移动及社交网络中分布式资源的开发利用》
《Android系统安全与攻防》
《内容分发网络》
《计算机网络仿真OPNET实用指南》
《移动无线信道》（原书第2版）
《LTE-Advanced：面向IMT-Advanced的3GPP解决方案》
《声学成像技术及工程应用》
《认知无线电通信与组网：原理与应用》
《LTE/SAE网络部署实用指南》
《网络性能分析原理与应用》
《云连接与嵌入式传感系统》
《IP地址管理原理与实践》
《自组织网络：GSM，UMTS和LTE的自规划、自优化和自愈合》
《实现吉比特传输的60GHz无线通信技术》
《LTE自组织网络（SON）：高效的网络管理自动化》
《UMTS中的LTE：向LTE-Advanced演进》（原书第2版）
《无线传感器及执行器网络》
《UMTS中的WCDMA－HSPA演进及LTE》（原书第5版）
《认知无线电网络》
《网络融合 ——服务、应用、传输和运营支撑》
《UMTS中的LTE:基于OFDMA和SC-FDMA的无线接入》
《高性能微处理器电路设计》
《吉规模集成电路互连工艺及设计》
《高级电子封装》（原书第2版）
《基于4G系统的移动服务技术》
《移动无线传感器网 ——技术、应用和发展方向》
《UMTS蜂窝系统的Q0S与Q0E管理》
《UMTS-HSDPA系统的TCP性能》
《基于射频工程的UMTS空中接口设计与网络运行》
《未来UMTS的体系结构与业务平台：全IP的3GCDMA网络》
《环境网络：支持下一代无线业务的多域协同网络》
《基于蜂窝系统的IMS—融合电信领域的V0IP演进》
《蜂窝网络高级规划与优化 2G/2.5G/3G/ ——向4G的演进》
《微电子技术原理、设计与应用》
《多电压CMOS电路设计》
《P2P系统及其应用》
《IPTV与网络视频：拓展广播电视的应用范围》
《下一代无线系统与网络》

WILEY







机械工业出版社微信服务号

上架指导　工业技术／通信技术



ISBN 978-7-111-48481-3　定价：59.80元